Exhibit 11 to Declaration of Mark C. Mao ISO Plaintiffs' Unopposed Motion for Final Approval of Class Action Settlement

David Boies (*pro hac vice* forthcoming)
dboies@bsfllp.com
BOIES SCHILLER FLEXNER LLP
333 Main Street
Armonk, NY 10504
Tel: (914) 749-8200

Mark C. Mao, CA Bar No. 236165
mmao@bsfllp.com
Beko Richardson, CA Bar No. 238027
brichardson@bsfllp.com
Joshua M. Stein, CA Bar No. 298856
jstein@bsfllp.com
BOIES SCHILLER FLEXNER LLP
44 Montgomery St., 41st Floor
San Francisco, CA 94104
Tel.: (415) 293-6800
Fax: (415) 293-6899

James Lee (*pro hac vice* forthcoming)
jlee@bsfllp.com
BOIES SCHILLER FLEXNER LLP
100 SE 2nd St., 28th Floor
Miami, FL 33131
Tel.: (305) 539-8400
Fax: (303) 539-1307

John A. Yanchunis (*pro hac vice* forthcoming)
jyanchunis@forthepeople.com
Ryan J. McGee (*pro hac vice* forthcoming)
rmcgee@forthepeople.com
MORGAN & MORGAN
201 N. Franklin Street, 7th Floor
Tampa, FL 33602
Tel.: (813) 223-5505

Michael F. Ram, CA Bar No. 104805
mram@forthepeople.com
MORGAN & MORGAN
711 Van Ness Ave, Suite 500
San Francisco, CA 94102
Tel: (415) 358-6913

Attorneys for Plaintiffs

SUPERIOR COURT OF CALIFORNIA
COUNTY OF SANTA CLARA

Gilbert Luna,
Isabella Massie,
Nico Westbrook,
Scott Daniels,
Steve Sonza,
Eugene Jackson,
Luke Russell,
Conor Gleeson,
Andrew Monheim,
Nicholas Dill,
Joseph Shofet,
Jerrell Jordon,
Joseph Brukner,
David Karvasales,
David Smalt,
Alexander Ely,
Ellen Dalen,
Ken Cornelius,

Case No. CaseNumber 24CV434093

COMPLAINT FOR DAMAGES

(1) VIOLATION OF CALIFORNIA'S INVASION OF PRIVACY ACT ("CIPA"), CAL. PENAL CODE §§ 631 & 632;
(2) VIOLATION OF THE COMPREHENSIVE COMPUTER DATA ACCESS AND FRAUD ACT ("CDAFA"), CAL. PENAL CODE §§ 502 ET SEQ.;
(3) INVASION OF PRIVACY;
(4) INTRUSION UPON SECLUSION;
(5) BREACH OF CONTRACT; AND
(6) VIOLATION OF CA UCL, CAL. BUS. & PROF. CODE §§ 17200, *ET. SEQ.*
(7) UNJUST ENRICHMENT

Steven Botosh,
Nichole Adams,
Johnathan Ornelas,
Brittany Powell,
Alain Mansoni,
Miranda Pierotti,
Kamari Quinones,
George Degraw,
Michael Nagle,
Julien Salgado,
Oliver Helms,
Nolan Dugger,
Omar Masri,
Ronald Corona,
Andrew Cardamone,
Keith Anderson,
Eijae Zanders,
Helena Apothaker,
Timothy Elliott,
Deana Steinberg,
Justin Nunez,
Anastasia Basche,
Andrea Cardona,
Alvaro Herrera,
Alberto Cuellar,
Abraham Valdez,
Alfredo Rodriguez,
Amir Chrayah,
Anthony Byrd,
Alan Starzinski,
Andrew Bith,
and Adeola Obasa,

Plaintiffs,

v.

GOOGLE LLC,

Defendant.

DEMAND FOR JURY TRIAL

TABLE OF CONTENTS

COMPLAINT

Plaintiffs file this Complaint against defendant Google LLC ("Google" or "Defendant"), and in support state the following.

INTRODUCTION

1. This lawsuit concerns Google's surreptitious interception and unlawful collection of Plaintiffs' personal and sensitive data while Plaintiffs were in "Incognito" mode in Google's Chrome browser, which was supposed to permit them to browse privately.

2. Google has represented to Google account holders, including Plaintiffs, that they are "in control of what information [they] share with Google," meaning that they have the power to limit what data Google tracks, collects, and shares with third parties. Google has represented that one way for users to exercise this "control" is by setting their web-browsing software (used to connect to websites) to "private browsing mode"—including Incognito mode in Google's Chrome browser ("Incognito"), which Google launched in 2008.

3. Based on Google's representations, Plaintiffs reasonably believed that their data would not be collected, stored, or used by Google and that Google would not intercept their communications when they were in "private browsing mode." This included Plaintiffs' Incognito mode visits to non-Google websites without being signed into any Google account.

4. Google's representations were and continue to be false. Google unlawfully intercepted Plaintiffs' private browsing communications to collect their personal and sensitive information, without disclosure or consent, including when they in Incognito mode visited non-Google websites without being signed into any Google Account.

5. Google has intercepted and collected Plaintiffs' private browsing data by causing their web browsing software to run Google software scripts (bits of code) that replicate and send the data to Google servers in California. These Google software "scripts" do this even if the user is in Incognito mode visiting non-Google websites. These Google software scripts give no notice to the user of Google's data collection methods, and operate without any choice or consent by users.

6. These same Google practices have been extensively litigated in a class action lawsuit filed in federal court in June 2020, where the federal court denied Google's motions to dismiss and

for summary judgment and also granted Rule 23(b)(2) certification for two nationwide classes seeking injunctive relief. *Brown v. Google LLC*, No. 4:20-cv-03664-YGR-SVK ("*Brown*" or the "*Brown* Lawsuit"), Dkts. 53, 82, 87, 89, 92, 113. Google previously represented and led users (and regulators) to believe—falsely—that users could limit Google's data collection practices by setting their Chrome browser to Incognito mode.

7. Admissions by Google employees found in many internal Google documents have become publicly available through the *Brown* Lawsuit, including for example:

- A 2014 Google email recommending changes to Incognito so "we don't deceive users."
- A Google email describing Incognito as "bad for users, bad for human rights, bad for democracy."
- A 2015 Google internal presentation regarding Incognito "misconceptions" noting "concern about Google collecting data in Incognito."
- A 2015 Google email describing Incognito as "radioactive" and "a lie."
- A 2016 Google email discussing Incognito and how "nothing will be more scannable than the name and icon, both of which are a poor fit for what the feature actually provides."
- A 2018 Google internal document titled "Five ways people misunderstand Incognito and private browsing" noting "common misconceptions" that could give a "false impression of privacy."
- A 2018 Google internal presentation titled "The Incognito Problem" noting Google branding and disclosures "confuse people" with Google "over-promising and under-delivering."
- A 2018 Google email discussing how the words "Incognito" and "private" reinforce the "misperception that your browsing is private everywhere instead of just on your device."
- A 2018 Google email stating "the blame for people's misconceptions about Incognito Mode is due to that name and branding" as "argued repeatedly."
- A 2019 Google internal document regarding Incognito stating "most users do not correctly understand the current messaging" and the need to clarify whether users are

"protected from Google."

- A 2019 Google internal document for CEO Sundar Pichai instructing him to not use the word "private" to describe Incognito due to "known misconceptions."
- A 2019 Google internal presentation noting Incognito "[u]sers currently believe that none of their data is collected and they are essential[ly] [sic] anonymous."
- A 2020 Google internal presentation noting private browsing users "do not understand how private mode works" with "several common misconceptions" including that it "hides browsing activity from Google."
- A 2020 Google internal document discussing Incognito and noting "[i]t's not private in ways that many users want, that is, as to Google" and "you don't have the ability to see or delete" data, "Google has it."
- A 2021 Google internal presentation noting Incognito "[u]sers overestimate the protections that Incognito provides and are unaware of the personalization and data collection that occurs."
- A 2021 email to Google CEO Sundar Pichai admitting Incognito is "not truly private."

8. Google accomplishes its surreptitious interception and data collection through means that include (without limitation) Google Analytics, Google "fingerprinting" techniques, concurrent Google applications and processes on a consumer's device, and Google's Ad Manager. More than 70% of all online publishers (websites) use one or more of these Google services. When a user's web-browsing software accesses one of those non-Google websites, hidden Google software "scripts" cause the user's device to send detailed, personal information to Google's servers, including the private browsing communications between the user and the website. This includes the contents of the webpage being requested and the URL viewed, by Plaintiffs, in Incognito mode.

9. Google's practices violate the law, infringe upon users' privacy, and give Google and its employees power to learn intimate details about individuals' lives, interests, and internet usage. This makes Google "one stop shopping" for any private, government, or criminal actor who wants to undermine individuals' privacy, security, and freedom.

10. Through its pervasive data tracking business, Google knows who your friends are,

what your hobbies are, what you like to eat, what movies you watch, where and when you like to shop, what your favorite vacation destinations are, what your favorite color is and even the most intimate and potentially embarrassing things you browse on the internet—regardless of whether you follow Google's advice to keep your activities "private." Notwithstanding consumers' best efforts, to keep their activities on the internet private, Google has made itself an unaccountable trove of information so detailed and expansive that George Orwell could never have dreamed it.

11. Plaintiffs are individuals who are all within the scope of the certified nationwide classes in the *Brown* Lawsuit who have now decided to separately seek monetary relief from Google based on Google's unlawful acts. Plaintiffs assert claims that already proceeded past motions to dismiss and summary judgment in the *Brown* Lawsuit, where the federal court certified two nationwide classes under Rule 23(b)(2) to pursue these claims for purposes of obtaining injunctive relief. Plaintiffs now each seek monetary relief from Google, including statutory damages. Google has taken the position that any request for monetary relief involves certain individualized issues and should be tried separately.

THE PARTIES

12. Plaintiffs are Google account holders whose internet use was tracked by Google while browsing the internet from the Chrome browser in Incognito mode. Plaintiffs assert claims arising from Google's knowing and unauthorized interception and tracking of their internet communications and activity and knowing and unauthorized invasion of consumer privacy.

13. Plaintiff Gilbert Luna ("Luna") is an adult domiciled in Imperial Beach, CA, who has an active Google account and during the relevant period used Incognito mode to visit non-Google websites without being signed in to any Google account.

14. Plaintiff Isabella Massie ("Massie") is an adult domiciled in Glendora, CA, who has an active Google account and during the relevant period used Incognito mode to visit non-Google websites without being signed in to any Google account.

15. Plaintiff Nico Westbrook ("Westbrook") is an adult domiciled in Arcata, CA, who has an active Google account and during the relevant period used Incognito mode to visit non-Google websites without being signed in to any Google account.

16. Plaintiff Scott Daniels ("Daniels") is an adult domiciled in Alameda, CA, who has an active Google account and during the relevant period used Incognito mode to visit non-Google websites without being signed in to any Google account.

17. Plaintiff Steve Sonza ("Sonza") is an adult domiciled in Rohnert Park, CA, who has an active Google account and during the relevant period used Incognito mode to visit non-Google websites without being signed in to any Google account.

18. Plaintiff Eugene Jackson ("Jackson") is an adult domiciled in Los Angeles, CA, who has an active Google account and during the relevant period used Incognito mode to visit non-Google websites without being signed in to any Google account.

19. Plaintiff Luke Russell ("Russell") is an adult domiciled in Huntington Beach, CA, who has an active Google account and during the relevant period used Incognito mode to visit non-Google websites without being signed in to any Google account.

20. Plaintiff Conor Gleeson ("Gleeson") is an adult domiciled in San Francisco, CA, who has an active Google account and during the relevant period used Incognito mode to visit non-Google websites without being signed in to any Google account.

21. Plaintiff Andrew Monheim ("Monheim") is an adult domiciled in Los Angeles, CA, who has an active Google account and during the relevant period used Incognito mode to visit non-Google websites without being signed in to any Google account.

22. Plaintiff Nicholas Dill ("Dill") is an adult domiciled in Stockton, CA, who has an active Google account and during the relevant period used Incognito mode to visit non-Google websites without being signed in to any Google account.

23. Plaintiff Joseph Shofet ("Shofet") is an adult domiciled in Los Angeles, CA, who has an active Google account and during the relevant period used Incognito mode to visit non-Google websites without being signed in to any Google account.

24. Plaintiff Jerrell Jordon ("Jordon") is an adult domiciled in Oakland, CA, who has an active Google account and during the relevant period used Incognito mode to visit non-Google websites without being signed in to any Google account.

25. Plaintiff Joseph Brukner ("Brukner") is an adult domiciled in Los Angeles, CA, who

has an active Google account and during the relevant period used Incognito mode to visit non-Google websites without being signed in to any Google account.

26. Plaintiff David Karvasales ("Karvasales") is an adult domiciled in San Francisco, CA, who has an active Google account and during the relevant period used Incognito mode to visit non-Google websites without being signed in to any Google account.

27. Plaintiff David Smalt ("Smalt") is an adult domiciled in Los Angeles, CA, who has an active Google account and during the relevant period used Incognito mode to visit non-Google websites without being signed in to any Google account.

28. Plaintiff Alexander Ely ("Ely") is an adult domiciled in Anaheim, CA, who has an active Google account and during the relevant period used Incognito mode to visit non-Google websites without being signed in to any Google account.

29. Plaintiff Ellen Dalen ("Dalen") is an adult domiciled in San Jose, CA, who has an active Google account and during the relevant period used Incognito mode to visit non-Google websites without being signed in to any Google account.

30. Plaintiff Ken Cornelius ("Cornelius") is an adult domiciled in Bakersfield, CA, who has an active Google account and during the relevant period used Incognito mode to visit non-Google websites without being signed in to any Google account.

31. Plaintiff Steven Botosh ("Botosh") is an adult domiciled in Hayward, CA, who has an active Google account and during the relevant period used Incognito mode to visit non-Google websites without being signed in to any Google account.

32. Plaintiff Nichole Adams ("Adams") is an adult domiciled in Cameron Park, CA, who has an active Google account and during the relevant period used Incognito mode to visit non-Google websites without being signed in to any Google account.

33. Plaintiff Johnathan Ornelas ("Ornelas") is an adult domiciled in Pasadena, CA, who has an active Google account and during the relevant period used Incognito mode to visit non-Google websites without being signed in to any Google account.

34. Plaintiff Brittany Powell ("Powell") is an adult domiciled in Glendora, CA, who has an active Google account and during the relevant period used Incognito mode to visit non-Google

websites without being signed in to any Google account.

35. Plaintiff Alain Mansoni ("Mansoni") is an adult domiciled in Dublin, CA, who has an active Google account and during the relevant period used Incognito mode to visit non-Google websites without being signed in to any Google account.

36. Plaintiff Miranda Pierotti ("Pierotti") is an adult domiciled in Richmond, CA, who has an active Google account and during the relevant period used Incognito mode to visit non-Google websites without being signed in to any Google account.

37. Plaintiff Kamari Quinones ("Quinones") is an adult domiciled in Oakland, CA, who has an active Google account and during the relevant period used Incognito mode to visit non-Google websites without being signed in to any Google account.

38. Plaintiff George Degraw ("Degraw") is an adult domiciled in Huntington Beach, CA, who has an active Google account and during the relevant period used Incognito mode to visit non-Google websites without being signed in to any Google account.

39. Plaintiff Michael Nagle ("Nagle") is an adult domiciled in Los Angeles, CA, who has an active Google account and during the relevant period used Incognito mode to visit non-Google websites without being signed in to any Google account.

40. Plaintiff Julien Salgado ("Salgado") is an adult domiciled in Martinez, CA, who has an active Google account and during the relevant period used Incognito mode to visit non-Google websites without being signed in to any Google account.

41. Plaintiff Oliver Helms ("Helms") is an adult domiciled in San Rafael, CA, who has an active Google account and during the relevant period used Incognito mode to visit non-Google websites without being signed in to any Google account.

42. Plaintiff Nolan Dugger ("Dugger") is an adult domiciled in Los Angeles, CA, who has an active Google account and during the relevant period used Incognito mode to visit non-Google websites without being signed in to any Google account.

43. Plaintiff Omar Masri ("Masri") is an adult domiciled in Long Beach, CA, who has an active Google account and during the relevant period used Incognito mode to visit non-Google websites without being signed in to any Google account.

44. Plaintiff Ronald Corona ("Corona") is an adult domiciled in San Francisco, CA, who has an active Google account and during the relevant period used Incognito mode to visit non-Google websites without being signed in to any Google account.

45. Plaintiff Andrew Cardamone ("Cardamone") is an adult domiciled in San Jose, CA, who has an active Google account and during the relevant period used Incognito mode to visit non-Google websites without being signed in to any Google account.

46. Plaintiff Keith Anderson ("Anderson") is an adult domiciled in Moss Beach, CA, who has an active Google account and during the relevant period used Incognito mode to visit non-Google websites without being signed in to any Google account.

47. Plaintiff Eijae Zanders ("Zanders") is an adult domiciled in Carson, CA, who has an active Google account and during the relevant period used Incognito mode to visit non-Google websites without being signed in to any Google account.

48. Plaintiff Helena Apothaker ("Apothaker") is an adult domiciled in West Hollywood, CA, who has an active Google account and during the relevant period used Incognito mode to visit non-Google websites without being signed in to any Google account.

49. Plaintiff Timothy Elliott ("Elliott") is an adult domiciled in Arcata, CA, who has an active Google account and during the relevant period used Incognito mode to visit non-Google websites without being signed in to any Google account.

50. Plaintiff Deana Steinberg ("Steinberg") is an adult domiciled in Stockton, CA, who has an active Google account and during the relevant period used Incognito mode to visit non-Google websites without being signed in to any Google account.

51. Plaintiff Justin Nunez ("Nunez") is an adult domiciled in Sacramento, CA, who has an active Google account and during the relevant period used Incognito mode to visit non-Google websites without being signed in to any Google account.

52. Plaintiff Anastasia Basche ("Basche") is an adult domiciled in Los Angeles, CA, who has an active Google account and during the relevant period used Incognito mode to visit non-Google websites without being signed in to any Google account.

53. Plaintiff Andrea Cardona ("Cardona") is an adult domiciled in Hemet, CA, who has

an active Google account and during the relevant period used Incognito mode to visit non-Google websites without being signed in to any Google account.

54. Plaintiff Alvaro Herrera ("Herrera") is an adult domiciled in San Jose, CA, who has an active Google account and during the relevant period used Incognito mode to visit non-Google websites without being signed in to any Google account.

55. Plaintiff Alberto Cuellar ("Cuellar") is an adult domiciled in Bellflower, CA, who has an active Google account and during the relevant period used Incognito mode to visit non-Google websites without being signed in to any Google account.

56. Plaintiff Abraham Valdez ("Valdez") is an adult domiciled in Chula Vista, CA, who has an active Google account and during the relevant period used Incognito mode to visit non-Google websites without being signed in to any Google account.

57. Plaintiff Alfredo Rodriguez ("Rodriguez") is an adult domiciled in Fullerton, CA, who has an active Google account and during the relevant period used Incognito mode to visit non-Google websites without being signed in to any Google account.

58. Plaintiff Amir Chrayah ("Chrayah") is an adult domiciled in Santa Ana, CA, who has an active Google account and during the relevant period used Incognito mode to visit non-Google websites without being signed in to any Google account.

59. Plaintiff Anthony Byrd ("Byrd") is an adult domiciled in Merced, CA, who has an active Google account and during the relevant period used Incognito mode to visit non-Google websites without being signed in to any Google account.

60. Plaintiff Alan Starzinski ("Starzinski") is an adult domiciled in Los Angeles, CA, who has an active Google account and during the relevant period used Incognito mode to visit non-Google websites without being signed in to any Google account.

61. Plaintiff Andrew Bith ("Bith") is an adult domiciled in Long Beach, CA, who has an active Google account and during the relevant period used Incognito mode to visit non-Google websites without being signed in to any Google account.

62. Plaintiff Adeola Obasa ("Obasa") is an adult domiciled in Redwood City, CA, who has an active Google account and during the relevant period used Incognito mode to visit non-

Google websites without being signed in to any Google account.

63. Defendant Google is a Delaware limited liability company with a principal place of business at what is officially known as The Googleplex, 1600 Amphitheatre Parkway, Mountain View, California 94043. Google regularly conducts business throughout California and in this judicial district. Google is one of the largest technology companies in the world and conducts product development, search, and advertising operations in this district.

JURISDICTION AND VENUE

64. This Court has jurisdiction because Google's principal place of business is in California, Google maintains its headquarters in Santa Clara County, California, and a substantial part of the events and conduct giving rise to Plaintiffs' claims occurred in this State, including Google's development of the at-issue technology and receiving, accessing, and using the intercepted communications and data at issue in California.

65. This Court is a proper venue for this action. Google is headquartered in and engaged in the unlawful conduct from this County, and the contract between Plaintiffs and Google includes a venue selection clause for Santa Clara County. Google's Terms of Service state "all disputes arising out of or relating to these terms, service specific additional terms, or any related services, regardless of conflict of laws rules ... will be resolved exclusively in the federal or state courts of Santa Clara County, California, USA, and you and Google consent to personal jurisdiction in those courts." Venue is therefore proper here in Santa Clara County.

FACTUAL ALLEGATIONS REGARDING GOOGLE

I. Google's History of Privacy Violations & Its Agreement with the FTC

66. Google's violation of consumers' privacy rights is not new—it has been persistent and pervasive for at least a decade.

67. In 2010, the FTC charged that Google "used deceptive tactics and violated its own privacy promises to consumers when it launched its social network, Google Buzz." To settle the matter, the FTC barred Google "from future privacy misrepresentations" and required Google "to

implement a comprehensive privacy program."[1]

68. In 2011, Google entered into a consent decree with the FTC (the "Consent Decree"), effective for 20 years, in which the FTC required and Google agreed as follows (emphasis added):

> IT IS ORDERED that [Google], in or affecting commerce, shall not misrepresent in any manner, expressly or by implication:
>
> A. the extent to which [Google] maintains and protects the privacy and confidentiality of any covered information, including, but not limited to, misrepresentations related to: (1) the purposes for which it collects and uses covered information, and (2) the extent to which consumers may exercise control over the collection, use, or disclosure of covered information.[2]

69. This requirement applies to the Google conduct at issue in this lawsuit, as the Consent Decree broadly defines "covered information" to include information Google "collects from or about an individual" including a "persistent identifier, such as IP address," and combinations of additional data with the same.

70. Just one year after the Consent Decree was entered, the FTC found that Google had already violated the Consent Decree, by way of Google's misrepresentations regarding what consumer data it would and would not collect with the Safari web browser. In an August 2012 press release, the FTC explained:

> Google Inc. has agreed to pay a record $22.5 million civil penalty to settle Federal Trade Commission charges that it misrepresented to users of Apple Inc.'s Safari Internet browser that it would not place tracking "cookies" or serve targeted ads to those users, violating an earlier privacy settlement between the company and the FTC.
>
> The settlement is part of the FTC's ongoing efforts make sure companies live up to the privacy promises they make to consumers, and is the largest penalty the agency has ever obtained for a violation of a Commission order. In addition to the civil penalty, the order also requires Google to disable all the tracking cookies it had said it would not place on consumers' computers.
>
> "The record setting penalty in this matter sends a clear message to all companies under an FTC privacy order," said Jon Leibowitz, Chairman of the FTC. "No matter how big or small, all companies must abide by FTC orders against them and keep their privacy promises to consumers, or they

[1] https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz.

[2] https://www.ftc.gov/sites/default/files/documents/cases/2011/03/110330googlebuzzagreeorder.pdf.

> will end up paying many times what it would have cost to comply in the first place."[3]

71. Since 2012, a number of federal, state, and international regulators have similarly accused Google of violating its promises to consumers on what data it would and would not collect, with Google failing to obtain consent for its conduct.

72. In September 2016, when Google updated its browser app for Apple iOS, Google wrote that users would have "[m]ore control with incognito mode" and "Your searches are your business. That's why we've added the ability to search privately with incognito mode in the Google app for iOS. When you have incognito mode turned on in your settings, your search and browsing history will not be saved."[4] Google made no statements about how users' privacy would actually be limited in these private browsing sessions and avoided for years what it now claims (as a result of this litigation shining the light on its practices): that users never had the privacy they were promised.

73. Similarly, in May 2018, Google modified its privacy policy to state, "[y]ou can use our services in a variety of ways to manage your privacy. . . . You can also choose to browse the web privately using Chrome in Incognito mode."[5]

74. Nonetheless, in 2019, Google and YouTube agreed to pay $170 million to settle allegations by the Federal Trade Commission and the New York Attorney General that YouTube video sharing services illegally collected personal information from children without their parents' consent.

75. Then, in June 2020, France's Highest Administrative Court upheld a 50 million Euro fine against Google based on its failure to provide clear notice and obtain users' valid consent to process their personal data for ad personalization purposes.

76. There have been myriad proceedings by the State Attorneys General and the

---

[3] https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented.

[4] https://www.googblogs.com/the-latest-updates-and-improvements-for-the-google-app-for-ios/. See also, https://search.googleblog.com/index.html.

[5] https://policies.google.com/privacy/archive/20171218-20180525?hl=en-US.

Australian Competition and Consumer Commission alleging Google's failure to obtain consent regarding its collection of location data and its decision to combine certain user data.

77. For example, in the Arizona Attorney General action, Google has produced documents establishing "overwhelming" evidence that "Google has known that the user experience they designed misleads and deceives users."

78. And in an Australia proceeding, the Australian Competition & Consumer Commission ("ACCC") alleged that "Google misled Australian consumers to obtain their consent to expand the scope of personal information that Google could collect and combine about consumers' internet activity, for use by Google, including for targeted advertising."[6] The ACCC contended that Google "misled Australian consumers about what it planned to do with large amounts of their personal information, including internet activity on websites not connected to Google."[7]

79. Google's employees made numerous admissions in internal communications, recognizing that Google's privacy disclosures are a "mess" with regards to obtaining "consent" for its data collection practices and other issues relevant in this lawsuit. Those documents are heavily redacted by Google, and include for example the following comments and questions by Google employees:

a. "Do users with significant privacy concerns understand what data we are saving?"

b. "[T]ake a look at [redacted by Google] – work in progress, trying to rein in the overall mess that we have with regards to data collection, consent, and storage."

c. "[A] bunch of other stuff that's super messy. And it's a Critical User Journey to make sense out of this mess."

---

[6] https://www.accc.gov.au/media-release/correction-accc-alleges-google-misled-consumers-about-expanded-use-of-personal-data#:~:text=The%20ACCC%20has%20launched%20Federal,Google%2C%20including%20for%20targeted%20advertising.

[7] *Id.*

80. Those internal documents are not limited to location data, and unredacted versions of those documents and other internal Google documents will further demonstrate and confirm the lack of consent for the Google conduct at issue in this lawsuit.

II. Google's Privacy Policy, Privacy "Controls," and "Incognito Screen" Each Falsely State that Users Can Prevent Google's Collection By Using "Private Browsing Mode" (Including Incognito Mode)

81. The public, legislators, and courts have become increasingly aware of online threats to consumer privacy—including threats posed by powerful technology companies like Google that have become household names.

82. To comply with the new laws like the California Consumer Privacy Act (the "CCPA") and Europe's General Data Privacy Regulation (the "GDPR") and to comply with the Consent Decree, Google has repeatedly represented that users have control over what information is shared with Google and that users can prevent Google from tracking their browsing history and collecting their personal data online.

83. Plaintiffs had a reasonable expectation of privacy while they were using a private browser mode. Specifically, Plaintiffs expected that, when they were using Incognito mode, Google (a) would not collect the data as described in this Complaint, and (b) would not thereafter use the data, collected during "private browsing mode," for all of the purposes described below.

84. This expectation of privacy was reasonable because of Google's own statements regarding "private browsing modes" like Incognito mode as described below, including the following:

- "***You're in control*** of what information you share with Google . . . ."
- "You can use our services in a variety of ways to manage your privacy . . . across our services, ***you can adjust our privacy settings to control what we collect and how your information is used.***"
- "You can also choose to ***browse the web privately*** using Chrome in Incognito mode."
- "Your search and ad results may be customized using search-related activity even if you're signed out. ***To turn off this kind of search customization, you can search***

and browse privately."

- "To browse the web privately, ***you can use private browsing,*** sign out of your account, change your custom results settings, or delete past activity."
- "Your searches are your business. . . . When you have incognito mode turned on in your settings, your search and browsing history ***will not be saved***."

Importantly, Google did not represent in any disclosure to Plaintiffs that it would continue to intercept, track, and collect communications even when they used a browser while in Incognito mode.

85. Google never notified Plaintiffs that Google would intercept, collect, store, or use Plaintiffs' communications while in Incognito mode.

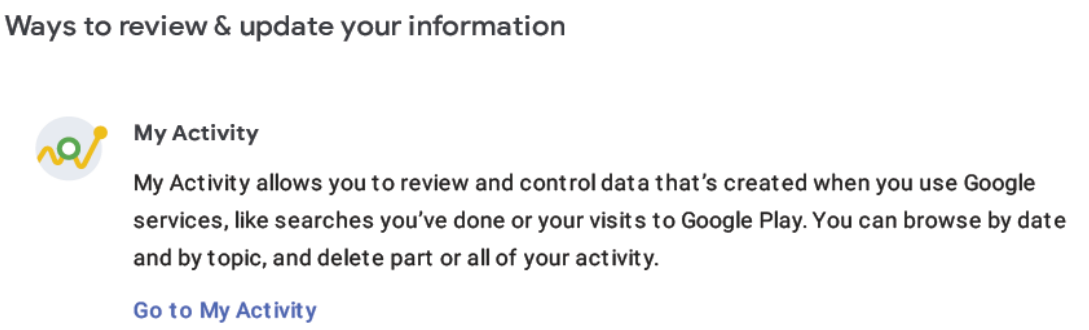
A. Privacy Policy

86. In Google's Privacy Policy (the "Privacy Policy"), Google made numerous representations about how users can "control" the information users share with Google and how users can browse the web anonymously and without their communications with websites being intercepted.

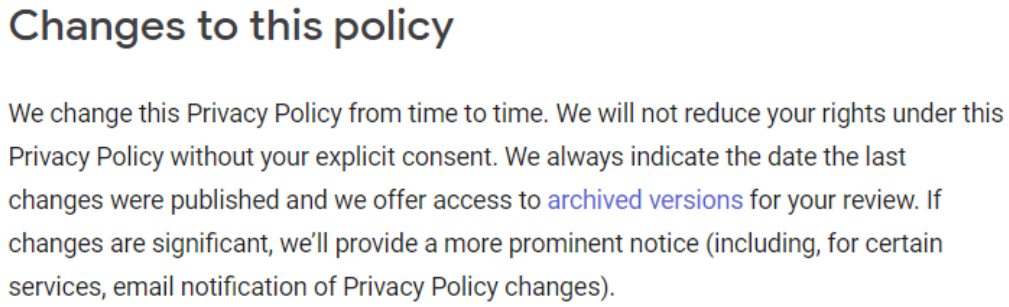
87. Google's Privacy Policy starts by stating in the Introduction section that "you can adjust your privacy settings to control what we collect and how your information is used" and that "[y]ou can choose to browse the web privately using Chrome in Incognito mode":

> on Google or watching YouTube videos. You can also choose to browse the web privately using Chrome in Incognito mode. And across our services, you can adjust your privacy settings to control what we collect and how your information is used.

88. The front and center of the "choices" offered to consumers is "Your privacy controls" on the Privacy Policy. Here, Google reiterates, "[y]ou have choices regarding the information we collect and how it's used." On the "My Activity" section of this part of the Privacy Policy, Google reiterates that "My Activity allows you to review and ***control data that's created when you use Google services,*** like searches you've done."



89. In the Privacy Policy Google also promises that it will not reduce the protections it guarantees to users without first obtaining their explicit consent to do so:



B. Privacy "Controls"

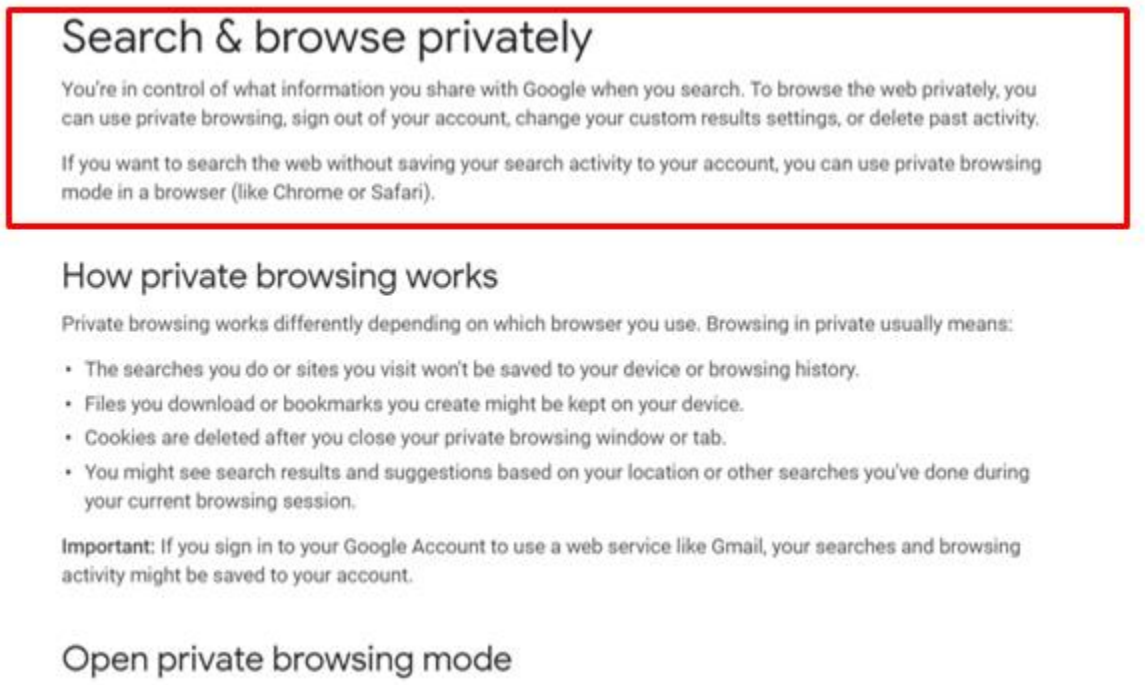
90. Users interested in controlling what Google collects are directed to the "Control Panel" of this same Privacy Policy, where Google assures users that "[t]o browse the web privately, you can use private browsing" and that "[i]f you want to search the web without saving your search activity to your account, you can use private browsing mode in a browser (like Chrome or Safari)."[8] When users click on "Go to My Activity" to control their data, they are presented with the option to "Learn more." When users click on "Learn more," they are taken to a page where they are supposed to be able to "View & control activity in your account." On that page, Google states that you may "[s]top saving activity temporarily. . . . You can search and browse the web privately," embedding a hyperlink to the "Search & Browse Privately" page.[9]

---

[8] https://support.google.com/websearch/answer/4540094?.

[9] *See* SEARCH & BROWSE PRIVATELY, https://support.google.com/websearch/answer/4540094?hl=en&ref_topic=3036132.

91. On the "Search & Browse Privately" page, Google once again reiterates that the user, not Google, is "in control of what information [a user] . . . share[s] with Google . . . ." Google states simply that consumers enabling "private browsing mode" on their browsers will allow consumers to "browse the web privately":



Search & browse privately

You're in control of what information you share with Google when you search. To browse the web privately, you can use private browsing, sign out of your account, change your custom results settings, or delete past activity.

If you want to search the web without saving your search activity to your account, you can use private browsing mode in a browser (like Chrome or Safari).

How private browsing works

Private browsing works differently depending on which browser you use. Browsing in private usually means:

- The searches you do or sites you visit won't be saved to your device or browsing history.
- Files you download or bookmarks you create might be kept on your device.
- Cookies are deleted after you close your private browsing window or tab.
- You might see search results and suggestions based on your location or other searches you've done during your current browsing session.

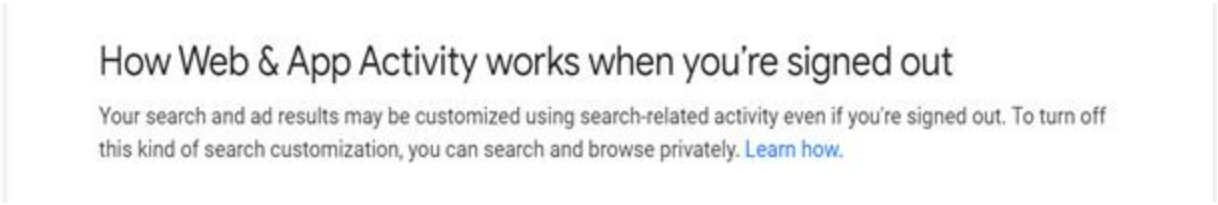
Important: If you sign in to your Google Account to use a web service like Gmail, your searches and browsing activity might be saved to your account.

Open private browsing mode

There is nothing on this page about Google Analytics, Google Ad Manager, any other Google data collection tool, or where and which websites online implement such data collection tools.

92. From the "View & control activity in your account" page referenced above, a consumer can also click the link, "See & control your Web & App Activity" on the right-hand side.[10] On that page, Google again represents that searching and browsing in "private browsing mode" will "turn off" any "search customization" "using search-related activity":

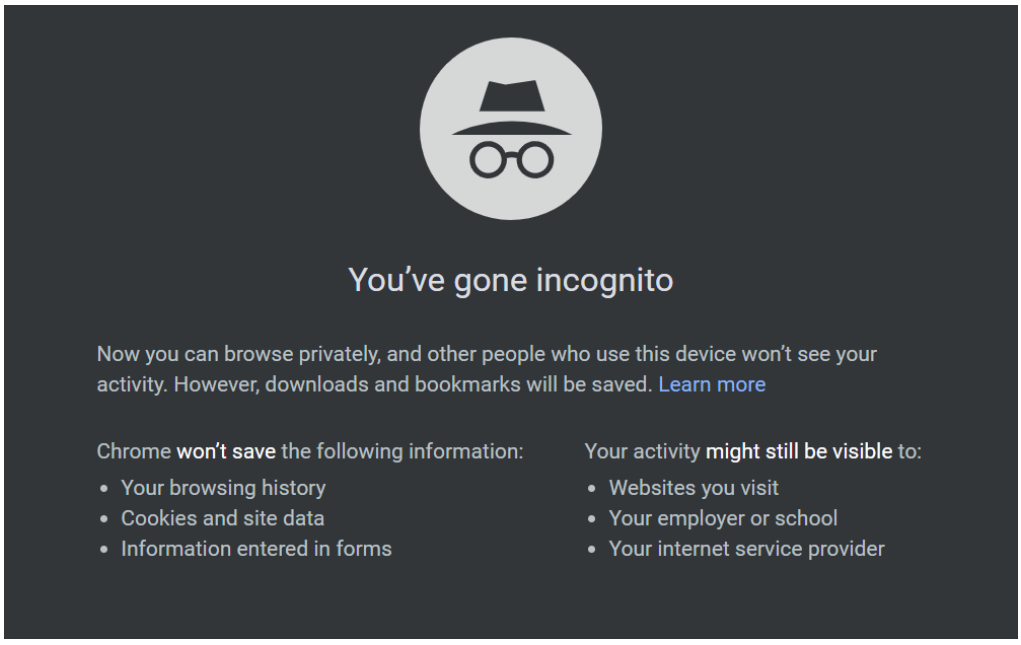
[10] SEE & CONTROL YOUR WEB & APP ACTIVITY, https://support.google.com/websearch/answer/54068?visit_id=637255508625725742210537612 8&hl=en&rd=1.



93. When users click the "Learn how" link, they are again redirected back to the "Search & Browse Privately" page. In other words, because Google repeatedly touts that users can "control" the information they share with Google and Google constantly refers users back to its recommendations on how users may "browse the web privately," users are left with only one reasonable impression—if they are searching or browsing the web in "private browsing mode," Google will honor their request to be left alone without further Google tracking.

C. "Incognito Screen"

94. "Incognito" is Google's name for the "private browsing mode" of Google's own web browser software, Google Chrome. Google has presented Plaintiffs and others with following splash screen (hereinafter the "Incognito Screen") when they start Incognito in Google's Chrome browser:



95. Based on these Google representations, Plaintiffs reasonably expected that Google would not collect their data while in Incognito mode. They reasonably understood "You've gone incognito" and "Now you can browse privately" to mean they could browse privately, without

Google's continued tracking and data collection. Google could have disclosed on this Incognito Screen that Google would track users and collect their data while they were browsing privately, but Google did not do that. Instead, Google included representations meant to assure users that they had "gone incognito" and could "browse privately" with only limited exceptions, none of which disclosed Google's own tracking and data collection practices while users were in a private browsing mode.

96. Google's Incognito Screen is also deeply misleading for three other reasons. ***First***, Google represents in the Incognito Screen that it "won't save . . . [y]our browsing history . . . cookies and site data[.]" False. In fact, Google's code continues to send the user's browsing history and other data directly to Google's servers during users' private browsing sessions. Google then associates that data with the user's "Google profile" across its services, so that Google can create, update, and monetize detailed profiles on billions of consumers.

97. ***Second***, Google represents in the Incognito Screen that "[n]ow you can browse privately, and other people who use this device won't see your activity." False. In fact, the session is not "private" at all, and "other people who use this device" will still know what preceding users did by way of targeted ads served by Google based on browsing activity that took place during the "private browsing."

98. ***Third***, Google represents in the Incognito Screen that the only entities to whom the user's "activity might still be visible" are "the websites you visit[,] [y]our employer or school[, and] [y]our internet service provider[.]" False. Users' activities are visible to Google, which continues to track users, intercept their communications, and collect their data while they are in Incognito mode and other private browsing modes.

99. What is conspicuously absent from the Incognito Screen—and any other representation by Google—is a disclosure that Google continues to track users while they are in a private browsing mode. Nothing in Google's Privacy Policy or Incognito Screen leads users to believe that during private browsing Google continues to persistently intercept their browsing data for its own profit. In fact, when the Privacy Policy and Incognito Screen are read together, the user necessarily reaches the opposite conclusion.

100. There are many other examples of Google representing that users could control what information was shared with Google, including by using a private browsing mode. For example, from May 2018 to February 2022, Google's Privacy Policy stated: "You can use our services in a variety of ways to manage your privacy. . . . You can also choose to browse the web privately using Chrome in Incognito mode." In September 2016, Google posted about an update for the Google app for iOS, stating that users would have "[m]ore control with incognito mode" and "Your searches are your business. That's why we've added the ability to search privately with incognito mode in the Google app for iOS. When you have incognito mode turned on in your settings, your search and browsing history will not be saved."

101. Google's representations about how it does not track users under these conditions are completely false, and contrary to the new privacy laws and its 2011 Consent Decree. Not only do consumers (including Plaintiffs) not know about what Google is doing to collect data on them, they have no meaningful way of avoiding Google's data collection practices, even if they are following Google's instructions to "browse the web privately."

D. Plaintiffs Had a Reasonable Expectation of Privacy

102. Plaintiffs' expectation of privacy was reasonable, not only because of Google's various representations, but also because of survey data showing the expectations of Internet users. A number of studies examining the collection of consumers' personal data confirms that the surreptitious taking of personal, confidential, and private information—as Google has done—violates reasonable expectations of privacy that have been established as general social norms. Privacy polls and studies uniformly show that the overwhelming majority of Americans consider one of the most important privacy rights to be the need for an individual's affirmative consent before a company collects and shares a subscriber's personal data. Indeed, a recent study by Consumer Reports shows that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing their data and the same percent believe internet companies and websites should be required to provide consumers with a complete

list of the data that has been collected about them.[11]

103. Just as importantly, since 2018, states like California passed the CCPA, which requires that data collection practices be disclosed at or before the actual collection is done.[12] Otherwise, "[a] business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section."[13]

III. Google Surreptitiously Intercepts Communications Between Users and Websites And Collects Personal and Sensitive User Data Even When the Users are in "Private Browsing Mode"

A. The Data Secretly Collected

104. Whenever Plaintiffs in Incognito mode visit a website that is running Google Analytics or Google Ad Manager, Google's software scripts on the website surreptitiously direct the user's browser to send a secret, separate message to Google's servers in California. This message contains:

a. The "GET request" sent from the user's computer or mobile device to the website. When an individual internet user visits a web page, his or her browser sends a message called a "GET request" to the webpage's server. The GET request serves two purposes: it first tells the website what information is being requested and then instructs the website to send the information back to the user. The copy of the "GET request," which is sent to Google, enables Google to learn exactly what content the user's browsing software was asking the website to display. The GET request also transmits a referer header containing the URL information of what the user has been viewing and requesting from websites online;

b. The IP address of the user's connection to the internet;[14]

---

[11] *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds,* CONSUMER REPORTS (May 11, 2017), https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety/.

[12] Cal. Civ. Section 1798.100(b). *See also*, Nev. Rev. Stat. Section 603A.340.

[13] *Id.*

[14] IP stands for "Internet Protocol." Each device, when connected to the Internet, is assigned a unique IP address by the Internet Service Provider (ISP) that is providing the internet connection. IP addresses may change over time but often do not. In many cases, an ISP will continue to assign the same IP address to the same device.

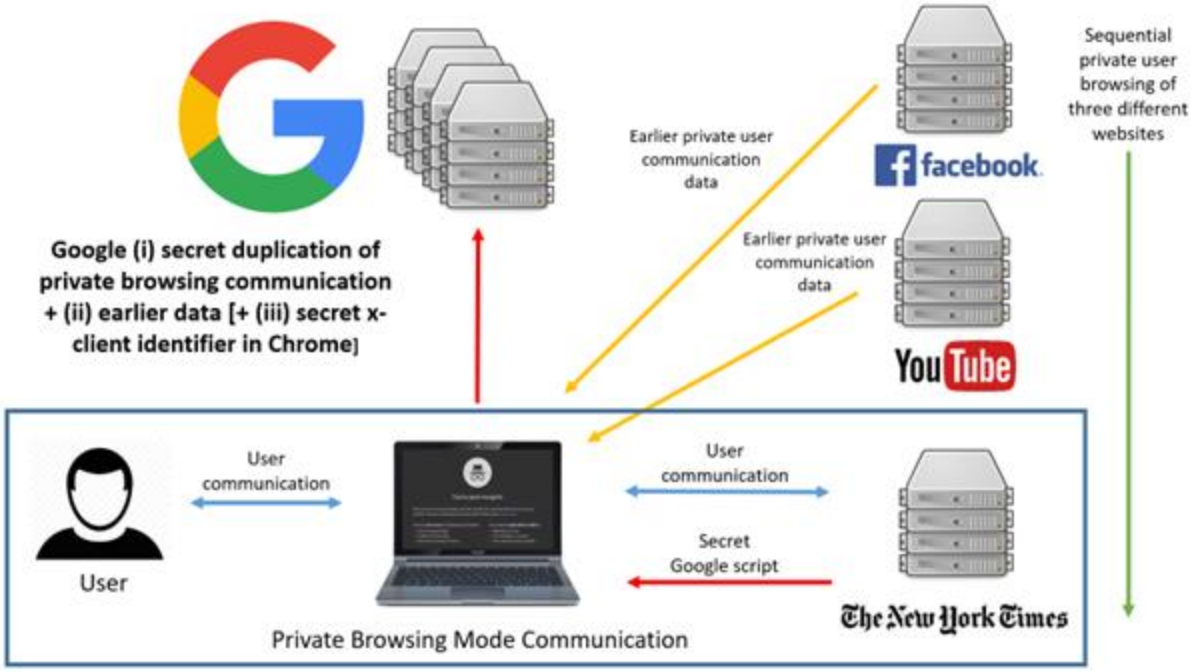
c. Information identifying the browser software that the user is using, including any "fingerprint" data (as described further below);

d. Any "User-ID" issued by the website to the user, if available (as described further below);

e. Geolocation of the user, if available (as described further below); and

f. Information contained in "Google cookies," which were saved by the user's web browser on the user's device at any prior time (as described further below).

105. To be clear, the second secret transmission directed by Google, containing both the duplicated message and additional data, is initiated by Google code and concurrent with the communications with the third-party website. This diagram illustrates the process:



106. The above chart illustrates how the user communicates with his or her own web browser in a private browsing mode, for example, by clicking on a link to content the user wishes to view on The New York Times. The user's browser then sends a communication to The New York Times. Because The New York Times is running Google Analytics, Google's embedded Google code, written in Javascript, sends secret instructions back to the user's browser, without alerting the user that this is happening. Google causes the user's browser to secretly duplicate the

communication with the website, transmitting it to Google servers in California. Google not only surreptitiously duplicates the data included in the communication with The New York Times but it also includes additional information on the user's prior private browsing histories with Facebook and YouTube, by way of technologies such as cached cookies from prior sessions. Where the user is using Google Chrome, Google also causes to be sent its X-Client-Data Header information if that is available, which uniquely identifies the user.

107. Google does not notify users of this secret Google software code designed to collect user data even while they are in a private browsing mode, which is hidden from users and run without any notice to users of the interception and data collection, which exceeded all contemplated and authorized use of their data. Users also have no way to remove that Google script or to opt-out of its functionality. Google designed the software in a way to render ineffective any barriers users may wish to use to prevent access to their information, including by browsing in Incognito mode or other private browsing modes. Private browsing modes are supposed to provide users with privacy, as represented by Google, but Google's software by design circumvents those barriers and enables Google to secretly collect user data and profile users.

B. Google Collects Data Using Google Analytics

1. Google Analytics Code

108. Over 70% of online websites and publishers on the internet, many of whom are businesses in California, utilize Google's website visitor-tracking product, "Google Analytics," in addition to other Google advertisement technology products (altogether the "Websites"). Google Analytics is a "freemium" service that Google makes available to websites.[15] Google Analytics provides data analytics and attribution about the origins of a Website's traffic, demographics, frequency, browsing habits on the Website, and other data about visitors. While Google Analytics is used by Websites, it is also essential to Google for its targeted advertisement services, and makes Google Search and its rankings possible by tracking the billions of visits to various Websites every

[15] Google Analytics is "free" to implement, but the associated data and attribution reports come at a price tag when Websites want more specific information. To obtain more specific and granular data about visitors, Websites must pay a substantial fee, such as by paying for Google's DV360, Ad Hub, or Google Audience products.

day.

109. To implement Google Analytics, Google requires that Websites embed Google's own custom but blackbox code into their existing webpage code. When a consumer visits a Website, his or her browser communicates a request to the Website's servers to send the computer script to display the Website. The consumer's browser then begins to read Google's custom code along with the Website's own code when loading the Website from the Website's server. Two sets of code are thus automatically run as part of the browser's attempt to load and read the Website pages—the Website's own code, and Google's embedded code. Google's embedded code causes the second and concurrent secret transmission from the user's browser (on the user's computer or other connected device), containing the duplicated message between the user and the Website, to be combined with additional data such as the user's prior browsing history and other Google trackers, to be sent to Google's servers.

2. User-ID

110. For larger websites and publishers that are able to pay Google's additional fees, Google offers an upgraded feature called "Google Analytics User-ID," which allows Google to map and match the user (including Plaintiffs) to a specific unique identifier that Google can track across the web. The User-ID feature allows Websites to "generate [their] own unique IDs, consistently assign IDs to users, and include these IDs wherever [the Websites] send data to Analytics." Because of Google's omnipresence on the web, the use of User-IDs can be so powerful that the IDs "identify related actions and devices and connect these seemingly independent data points. That same search on a phone, purchases on a laptop, and re-engagement on a tablet that previously looked like three unrelated actions on unrelated devices can now be understood as one user's interactions with [the website's] business."[16] This User-ID information is even more useful to Google than the individual websites, however. Across millions of websites, Google is able to use its secretly embedded computer scripts and User-IDs to compile what URLs the same users are viewing, even when they are in "private browsing mode," adding all of this information to

[16] *How USER-ID Works*, Google Analytics Help, https://support.google.com/analytics/answer/3123662?hl=en&ref_topic=3123660.

Google's stockpile of user profiles. In short, with its market power and User-IDs, no one else can track users online like Google.

3. Cookies

111. Google also uses various cookies (hereinafter "Cookies") to supplement Google Analytics' tracking practices. Specifically, Google Analytics contains a script that causes the user's (including Plaintiffs') browser to transmit, to Google, information from each of the Google Cookies already existing on the browser's cache. These Cookies typically show, at a minimum, the prior websites the user has viewed.[17] These Cookies help enrich Google's profile on the user, which Google uses for its own benefit and profit.

112. Google typically has its Cookies working with Google Analytics coded as "first party cookies,"[18] so that consumers' browsers are tricked into thinking that those Cookies are issued by the Website and not Google. This makes it very difficult for consumers to block Google's Cookies, even if consumers tried to block or clear the cookies issued by "third parties."

113. As discussed earlier, Google's misuse of Cookies on the Safari browser to circumvent user controls was exactly what caused the FTC to fine Google $22.5 million in 2012. The FTC had found that such circumvention of consumer controls and representations were direct violations of the Consent Decree.

4. No Consent

114. Google, as a matter of policy, does not require that Websites disclose how Google Analytics work to consumers (including Plaintiffs). Also, Google does not tell its users which websites implement Google Analytics. Google starts collecting user data as soon as a page is loading, before a consumer even had the chance to review the page. There is no effective way for

---

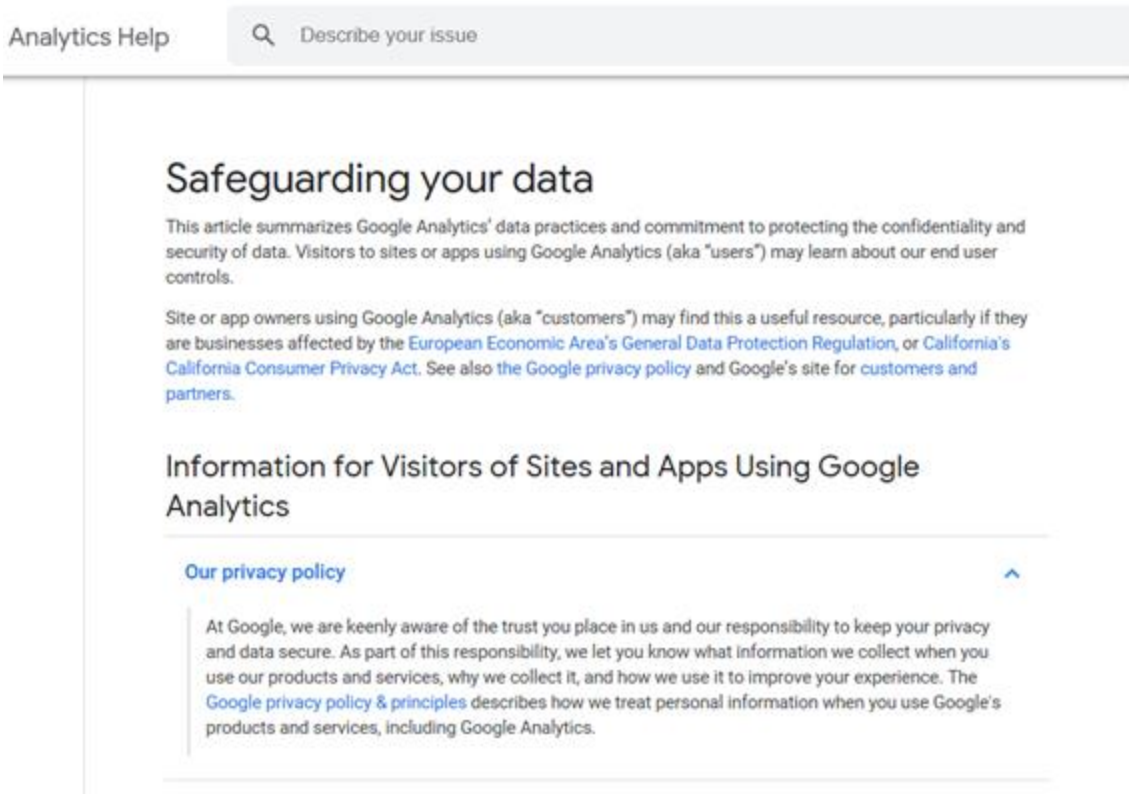
[17] A "cookie" is a piece of code that records information regarding the state of the user's system (e.g., username; other login information; items added to a "shopping cart" in an online store) or information regarding the user's browsing activity (including clicking particular buttons, logging in, or recording which pages were visited in the past). Cookies can also be used to remember pieces of information that the user previously entered into form fields, such as names, addresses, passwords, and payment card numbers. Even in "private browsing mode," Google's "scripts" on websites cause the user's browser to transmit information to Google relating to pre-existing "cookies" on the user's system.

[18] https://developers.google.com/analytics/devguides/collection/analyticsjs/cookie-usage

users to avoid Google Analytics along with Google's secret interceptions and data collection. Where users have not been presented with an actual choice, there can be no consent.

115. Websites implementing Google Analytics do not consent to the Google conduct at issue in this lawsuit, where Google collects consumer data for Google's own purposes and financial benefit while users have enabled Incognito mode. Google never receives consent from Websites implementing Google Analytics or otherwise that Google may continue to intercept user activity and user data for its own purposes even when Incognito mode has been enabled.

116. Google's disclosures confirm the lack of consent from Websites to intercept or collect data while users are in Incognito mode. Google represents to consumers and Websites alike that Google will adhere to its own Privacy Policy as represented, whenever Google Analytics is used. Specifically, Google states on the Analytics Help page for Websites the following, regarding how it follows its own Privacy Policy:



When any Website clicks on the "Google privacy policy & principles" above, they are taken to Google's Privacy Policy homepage at https://policies.google.com/privacy?hl=en, where Google has made assurances to the users such as "you can adjust your privacy settings to control what we collect and how your information is used" and that "[y]ou can choose to browse the web privately using Chrome in Incognito mode." In short, Google has assured Websites that Google Analytics will only be implemented on Websites in such a way that individual users maintain control.

117. Accordingly, Websites implementing Google Analytics have not consented, do not consent and cannot consent to Google's interception and collection of user data for Google's own purposes when users have enabled Incognito mode because doing so would violate Google's own Privacy Policy, as well as its assurances that its product complies with privacy laws and the Consent Decree by respecting consumer choice.

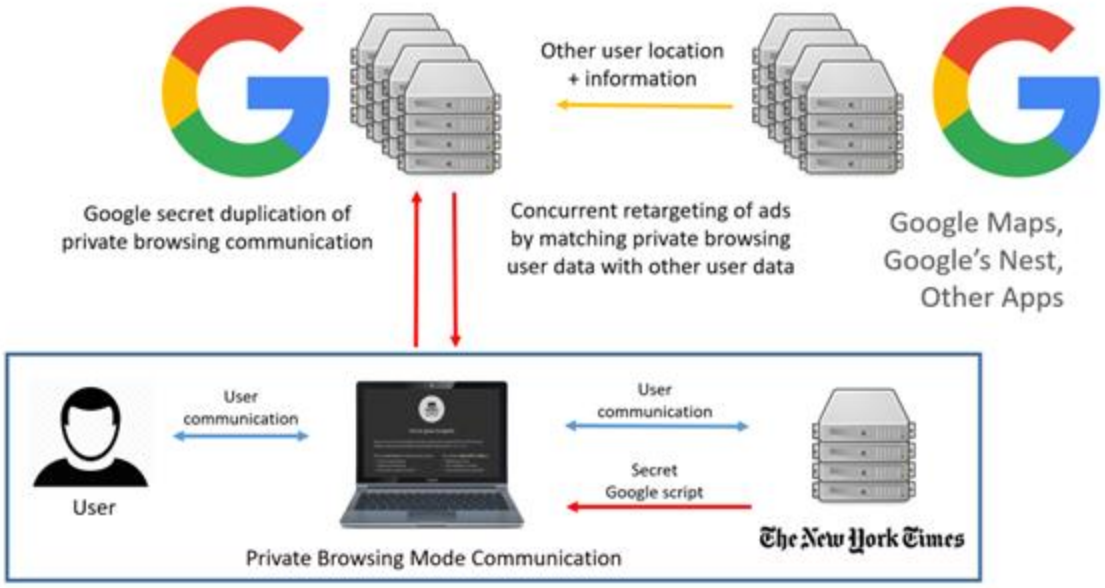
C. Google Collects Data Using Ad Manager

118. In addition to Google Analytics, over 70% of website publishers, many of whom are businesses in California, utilize another Google tracking and advertising product, called "Google Ad Manager" (formerly known as "DoubleClick For Publishers" or "DFP"), which also collects the users' URL viewing history.

119. Like Google Analytics, Google Ad Manager requires Google code to be embedded into the Website's code. When the user's (including Plaintiffs) browser sends a communication to the website, asking for content to be displayed (i.e., the URL), then the embedded Google code causes the user's browser to display targeted Google advertisements. These targeted ads are displayed along with the Website's actual content. These advertisements are shown to the user on behalf of Google's advertising customers, allowing Google to make money.

120. Google Ad Manager also uses Approved Pixels (*supra*) and Cookies to track users across the internet. Because of the number of Websites that use Google Ad Manager, it is very difficult for consumers (including Plaintiffs) to avoid its persistence. Like Google Analytics, Google Ad Manager begins collecting information on a user, before the content for the webpage has even fully loaded.

121. To maximize Google's revenue, Google Ad Manager is set up to automatically retarget a user based on information that Google has previously collected, whether this information is based on a persistent identifier (e.g., Google Analytics User-ID, X-Client-Data Header, *supra*), Google's fingerprinting (e.g., Approved Pixels, *supra*), or geolocation. Thereafter, Google continues to track and target the same user across the internet:



122. In many cases, the intercepted communications provide the "context" for targeted "contextual advertising" for Google, where Google combines the URL the consumer is viewing, with what Google knows about that user (e.g., Google Analytics User-ID, geolocation), to target the consumer in the "context" of his or her web experience. Because of Google's pervasive presence on the internet, its unparalleled reach and its uncanny ability to so target consumers, advertisers are willing to pay a premium for Google's advertisement services.

123. As with Websites implementing Google Analytics, Websites using Ad Manager do not consent to Google collecting data for Google's own purposes while users have enabled Incognito mode. On information and belief, Google never receives consent from Websites implementing Ad Manager that Google may continue to intercept user activity and user data for its own purposes when Incognito mode has been enabled. Indeed, Google represents to consumers

and Websites alike that it will adhere to its own Privacy Policy.[19]

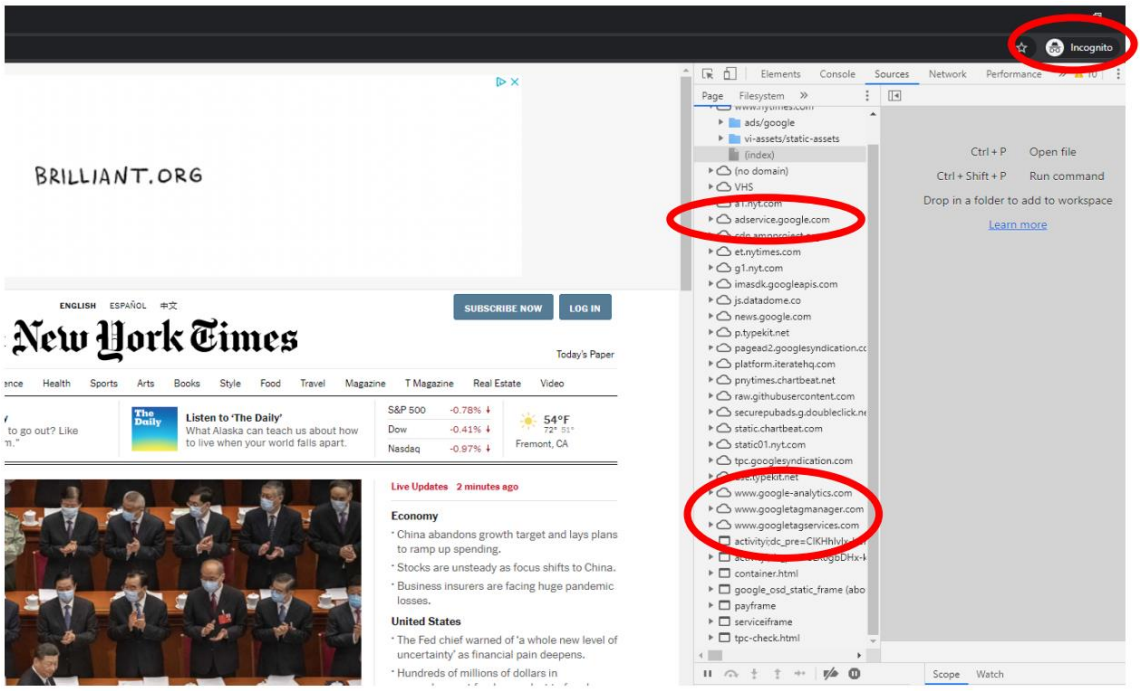
D. Google Collects This Data From Users Even in Incognito Mode

124. All of the Google data collection, described above, continues to occur when a user (including Plaintiffs) enters Incognito mode on the user's Chrome browser software. Specifically, Google intercepts the communications between the user and the Websites, whenever the user requests any page from the Website, thereby communicating and requesting a specific URL. Google then duplicates this communication and causes it to be sent to its own servers, after pairing the intercepted communications with whatever other data it can collect, so that Google can generate and profit from targeted advertisements.

125. There is no disclosure or consent associated with this Google interception and data collection, as Google designed its software code to run secretly, without disclosure, and render ineffective users' efforts to restrict Google's interception and data collection. Google was never authorized to take and use the information it obtained while users were in Incognito mode, where users revoked any rights Google might otherwise have had to collect such data.

126. Take, for example, someone who visits *The New York Times* website in private mode with his Google Chrome browser. Even when he is browsing with "private browsing mode" enabled, Google Analytics and Google Ad Manager continue to track his data. This is demonstrated by the following screenshot, which is not presented to the user and accessible only by using developer tools:

[19] https://policies.google.com/privacy?hl=en.



127. As described above, Google's secret Javascript code from Google Analytics causes the user to concurrently send to Google not only a duplicated copy of the communications requesting the webpage with the Website but also additional data from the browser, such as Cookies, browser information and the X-Client-Referrer Header if it is available. And Google's Ad Manager not only intercepts the user's communications with the Websites; it concurrently combines the duplicated communications as soon as the user loads a webpage, with data from other Google processes to target the user with advertisements based on the combined information.

128. Thus, even when users are browsing the internet in "private browsing mode," Google continues to track them, profile them and profit from their data whenever they visit a Website that uses Google Analytics or Google Ad Manager. Google collects precisely the type of private, personal information users wish and expect to protect when they have taken these steps to control what information is shared with Google. Google's tracking occurred and continues to occur no matter how sensitive or personal users' online activities are.

IV. Google Creates Profiles On Its Users Using Confidential Information

A. Google's Business Model Requires Extensive And Continual User Data Collection

129. The core of Google's business model is targeted advertising. In fact, the bulk of

Google's hundreds of billions of dollars in revenue annually come from what companies pay Google for targeted advertising,[20] both on Google Search and on various websites and applications that use Google services. The more accurately that Google can track and target consumers, the more advertisers are willing to pay Google's high advertisement fees and services.

130. Allowing consumers (including Plaintiffs) control over Google's data collections and ad targeting—with an ability to stop Google's data collections and ad targeting, including while in a private browsing mode—is actually against Google's interests and Google's track record with regulators worldwide prove that Google is always tempted to play fast and loose with its obligations and efforts to continue its data collection and ad targeting.

131. Because Google has already collected detailed "profiles" on each user and their devices, Google (with its algorithms, machine learning, and artificial intelligence apparatus) is able to associate the data (collected from users in private browsing mode) with those users' pre-existing Google "profiles." Doing so improves the "profiles" and allows Google to sell more targeted ads at those users, among many other uses.

B. Google Creates a User Profile on Each Individual

132. Google strives to build "profiles" on each Plaintiff and each of their devices. These "profiles" contain all the data Google can collect associated with each individual.

133. By tracking, collecting and intercepting users' (including Plaintiffs') personal communications indiscriminately—regardless of whether users attempted to avoid such tracking pursuant to Google's instructions—Google has gained a complete, cradle-to-grave profile of users:

a. In many cases, Google is able to associate the data collected from users in "private browsing mode" with specific and unique user profiles through Google Analytics User-ID. Google does this by making use of a combination of the unique identifier of the user it collects from Websites, and Google Cookies that it collects across the internet on the same user;

---

[20] https://www.investopedia.com/articles/investing/020515/business-google.asp#:~:text=Google%20Ads%20and%20Search%20Advertising,results%20generated%20by%20Google's%20algorithm.

b. Information collected from Google Cookies, which includes identifying information regarding the user from private browsing sessions and non-private browsing sessions, across multiple sessions;

c. Identifying information regarding the consumer from various Google fingerprinting technologies that uniquely identify the device, such as X-Client-Data Header, GStatic, and Approved Pixels;

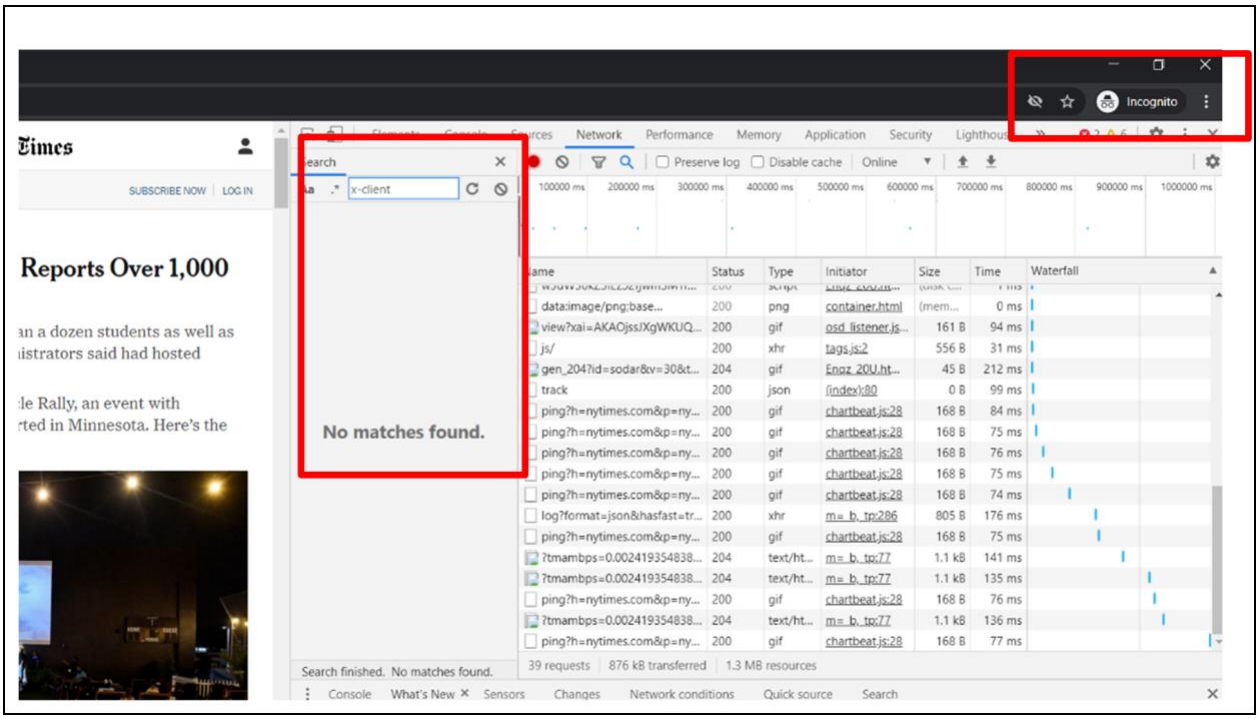
d. Geolocation data that Google collects from concurrent Google processes and system information, such as from the Android Operating System; and

e. The IP address information, which is transmitted to Google's servers during the private and non-private browsing sessions. Google correlates and aggregates all of this information to create profiles on the consumers.

C. Google Analytics Profiles Are Supplemented by the "X-Client-Data Header"

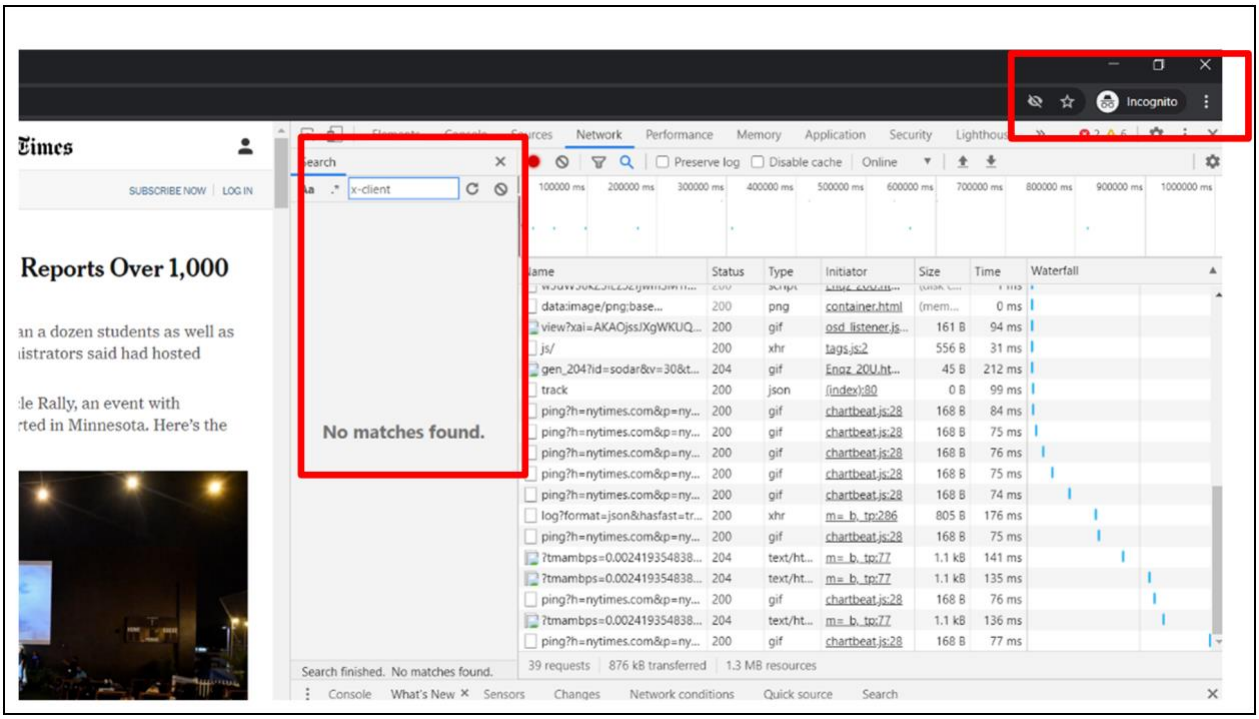
134. Another powerful tool Google uses in building detailed profiles of what may someday be every individual on the planet is the X-Client-Data Header.

135. Google's Chrome browser identifies every device upon the first installation of Chrome with a unique digital string of characters called Google's "X-Client-Data Header," such that Google uniquely identifies the device and user thereafter. Whenever Chrome is used, the Google browser is constantly transmitting this X-Client-Data Header to Google servers. Developer tools confirm this as follows:



136. Through the X-Client-Data Header, by itself or in combination with other Google identifiers, Google is able to tell whether a user (including Plaintiffs) is in Incognito mode or not. The X-Client Data Header is present in all Chrome-states except when the user is in Incognito mode.[21] Developer tools confirm this as follows:

[21] Consistent with its historical behavior, Google actually tried to turn on the X-Client-Data Header for users in March 2020, but was called out by Microsoft engineers on technical forums. https://bugs.chromium.org/p/chromium/issues/detail?id=1060744&q=x-client-data&can=1&mode=grid&start-date=2020-04-23&end-date=2020-05-23&x=Target. Google thereafter called it a "bug," and reverted the browser back to not transmitting the identifier when the user is in Incognito. As Plaintiffs will prove, however, Google was concurrently representing to the press at this time that Google was not so using the X-Client-Data Header in Incognito, when in fact it was. *See, e.g.*, https://www.theregister.co.uk/2020/03/11/google_personally_identifiable_info/.



137. The X-Client-Data Header allows Google to track Chrome users across the web, because it remains unchanged even if users "clear their browser cache" of cookies.[22]

138. Like Cookies, when the X-Client-Data Header is available, Google will concurrently collect this identifier with the duplicated communications it gets from the Websites and browser, to make it near impossible for the consumer to escape Google's surveillance.

139. Google designed the Chrome browser software to track users, which further renders ineffective users' efforts to prevent Google's access to their information and Google's creation of detailed user profiles for Google's advertising and profits.

D. Google Identifies You with "Fingerprinting" Techniques

140. Google also builds its profile of users (including Plaintiffs) by "fingerprinting" techniques. Because every device and application installed has small differences, images, digital pixels, and fonts display differently for every device and application, just ever so slightly. By forcing a consumer to display one of its images, pixels, or fonts, online companies such as Google

[22] *See* Thomas Claburn, *Is Chrome Really Secretly Stalking You Across Google Sites Using Per-Install ID Numbers? We Reveal the Truth*, THE REGISTER (Feb. 5, 2020), https://www.theregister.co.uk/2020/02/05/google_chrome_id_numbers/.

are able to "fingerprint" their users and consumers across the internet, with or without their permission.

141. For example, a large portion of the Websites also use Google's GStatic, which is a Google-hosted service for fonts, where Google loads the fonts displayed on the Website, instead of the Website's web server. Google sells this service as something that allegedly helps to reduce bandwidth and improve loading time, because Google is hosting the fonts. Plaintiffs are informed and believe and on that basis allege that GStatic is an additional way that Google identifies and tracks consumers, including when consumers are using a private browsing mode.

142. Google also authorizes Websites to place digital pixels ("Google Approved Pixels") embedded within the Websites' code.[23] These pixels are typically created and maintained by "approved third parties" (such as comScore, a data broker registered with California's CCPA data broker registry).

143. Again, when a user's web browser accesses a website containing a Google Approved Pixels, that browser responds to the pixel by generating a unique display. Each user's display is unique because it is generated in part, from certain digital signatures that are unique to each specific device (in combination with the browser software running on the device). By tracking these pixels and the unique resulting displays, Google and its data-broker partners are able to track and "measure" consumers across the web.

144. GStatic and Google Approved Pixels enable Google to identify consumers because the way the fonts and pixels are displayed on the browser help to uniquely identify whom the user is. This again is another set of data surreptitiously collected by Google vis-à-vis the consumer's browser which is added to the duplicated communications between the user and Websites, which Google collects concurrent with the user's communications with the Website even when users are in a private browsing mode.

E. Google Identifies You With Your System Data and Geolocation Data

145. Google also collects additional system data and geolocation data from (a) the

[23] *See, e.g.*, USE TRACKING PIXELS, https://support.google.com/news/publisher-center/answer/9603438?hl=en, describing partnership with comScore.

Android operating system running on users' phones or tablets and (b) Google applications running on phones (e.g., Chrome and Maps), Google Assistant, Google Home, and other Google applications and services.

146. Google collects information for its user profiles (including Plaintiffs) by making use of (a) the Android operating system, which Google created and makes available for smart phones, and (b) various Google applications that run on mobile devices. In a 2018 white paper entitled "Google Data Collection,"[24] Professor Douglas C. Schmidt of Vanderbilt University concluded that Google's Android operating system, and several of Google's mobile applications, are constantly sending system and location data to Google's servers. Specifically, Professor Schmidt wrote:

> Both Android and Chrome send data to Google even in the absence of any user interaction. Our experiments show that a dormant, stationary Android phone (with Chrome active in the background) communicated location information to Google 340 times during a 24-hour period, or at an average of 14 data communications per hour. In fact, location information constituted 35% of all the data samples sent to Google.

Indeed, now that Google has acquired Nest and merged Nest's data with data obtained via Google Home, Professor Schmidt's analysis regarding Google's ability to identify and track who and where we are is even more persistent and pernicious.

147. When any user of a Nest or Google Home product is running a Nest or Google Home application, concurrent with Google Assistant, Google is using the data collected from those processes to target users for advertisements. To optimize those advertisements, Google collects the user's geolocation.

148. Because Google Assistant and other Google applications are constantly tracking your geolocation, Google knows exactly who you are, regardless of whether you are in "private browsing mode" on the web, and Google is collecting and profiting from that personal user data.

149. In a *Wired* article regarding Google's privacy practices, Professor Schmidt stated

---

[24] Douglas C. Schmidt, *Google Data Collection*, DIGITAL CONTENT NEXT 1 (Aug. 15, 2018), https://digitalcontentnext.org/wp-content/uploads/2018/08/DCN-Google-Data-Collection-Paper.pdf.

that Google's "business model is to collect as much data about you as possible and cross-correlate it so they can try to link your online persona with your offline persona. This tracking is just absolutely essential to their business. 'Surveillance capitalism' is a perfect phrase for it."[25] By collecting increasing amounts of user data, Google is able to leverage such data to grow its third-party advertising business and profit.

150. Plaintiffs are informed and believe that all of this Google data collection happens even when a consumer is in the web browser's "private browsing mode." Indeed, the Arizona Attorney General alleged that Google deceptively tracks users based on various sources of location data, overriding consumer privacy controls and preferences.[26]

151. Plaintiffs are informed and believe that Google has contended in private industry conversations and in internal meetings and documents, that such surreptitious data collection is permissible, as it "aggregates the data" after the data has already been intercepted, collected, reviewed, and analyzed by Google. Even if that contention were true, that would not excuse Google's unlawful interceptions of data from users in "private browsing mode."

152. Plaintiffs are informed and believe that Google has also claimed in private industry conversations and in internal meetings and documents that its data collection practices are acceptable and not impermissible interceptions of communications, because Google is "acting on behalf of the website(s)", as their vendor. This contention is untrue. As the chart above indicates, Google's secret embedded code causes the user data to be sent directly to Google's servers in California. Google then treats that user data as Google's own property, which Google may use or sell as it pleases. Indeed, for a website to get access to the data that Google has collected using the embedded code running on that website, the website's publisher must pay a premium price to Google.

V. Google Profits from Its Surreptitious Collection of User Data

153. Google's continuous tracking of users is no accident. Google is one of the largest

---

[25] Lily Hay Newman, *The Privacy Battle to Save Google from Itself*, WIRED (Nov. 1, 2018), https://www.wired.com/story/google-privacy-data/.

[26] *See* Complaint, *Arizona v. Google LLC,* Arizona Sup. Ct. Case No. 2020-006219 (May 27, 2020).

technology companies in the world. Google LLC and its parent Alphabet Inc. have over 1.8 billion active account users, and Alphabet Inc. boasts a net worth exceeding $1.5 trillion.

154. Google's enormous financial success results from its unparalleled tracking and collection of personal and sensitive user information (including Plaintiffs') and selling and brokering of that user information to optimize advertisement services. Recently, virtually all of Google's revenue was attributable to third party advertising and it is continuously driven to find new and creative ways to leverage its access to users' data in order to sustain its phenomenal growth.

155. Google profits from the data it collects—including the user data collected while users are in a private browsing mode—in at least three ways. First, Google associates the confidential communications and data with a user profile or profiles, to enrich Google's ability to charge its customers for advertisement-related services. Second, Google later uses the intercepted confidential communications and user data (in combination with the user's profile) to direct targeted advertisements to consumers (including Plaintiffs). Third, Google uses the results to improve Google's own algorithms and technology, such as Google Search.

156. The data Google collects contains consumers' personal viewing information. Google collects, reads, analyzes the contents of, and organizes this data based on consumers' prior histories. Google creates "profiles" for each individual user and/or each individual device that accesses the Internet. Google seeks to associate as much information as possible with each profile because, by doing so, Google can profit from Google's ad-targeting services.

157. For example, Plaintiffs are informed and believe and on that basis allege, that Google often demands that websites pay for significant and expensive upgrades (e.g., such as to Google's DV360) in order for the Websites to obtain access to specific visitor information. That Google holds such detailed information regarding visitors hostage is proof that Google collects consumer information on Websites primarily for its own use and profit.

158. Likewise, Google Ad Manager is a service that generates targeted advertisements to be displayed alongside third-party websites' content. The user profiles, which Google creates and maintains using the collected user data, are used by Google's algorithms to select which ads to display through Google.

159. Google is paid for these advertisements by the third-party advertisers. Google is able to demand high prices for these targeted-advertising services because Google is able to use user profiles (including data that Google obtained from users while in "private browsing" mode) to select and display advertisements targeted at those specific profiles.

160. Plaintiffs are informed and believe that Google also benefits by using the data it collects to improve and refine existing Google products, services, and algorithms and also to develop new products, services and algorithms. This collection, usage, or monetization of user data contravenes the steps Plaintiffs have taken to try to control their information from being tracked or used by Google in any way, for Google's own profits.

161. Google market power in Search is entirely dependent on its ability to track what consumers are doing. The trackers that Google has across the internet not only tell Google where consumers go subsequent to searching on Google Search, the trackers allow Google to track what websites are popular and how often they are visited. By compiling not just consumer profiles, but surveying human behavior across the vast majority of web browser activity, Google is able to create a better and more effective search product as compared to its competitors, by its ability to claim that Google knows how to best rank websites and online properties, because Google can track consumer activity better than anyone else. Google Search would not be nearly as effective of a search tool without Google Analytics as a complement.

162. Google profits from users by acquiring their sensitive and valuable personal information, which includes far more than mere demographic information and volunteered personal information like name, birth date, gender and email address. More importantly, when consumers use Google, Google secretly plants numerous tracking mechanisms on users' computers and web-browsers, which allow Google to track users' browsing histories and correlate them with user, device, and browser IDs, rendering ineffective users' efforts to prevent access to their data.

163. The information Google tracks has and had massive economic value. This value is well understood in the e-commerce industry, and personal information is now viewed as a form of currency.

164. Well before the *Brown* Lawsuit, there was a growing consensus that consumers'

sensitive and valuable personal information would become the new frontier of financial exploit.

165. Professor Paul M. Schwartz noted in the *Harvard Law Review*:

> Personal information is an important currency in the new millennium. The monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from the trend. Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information.[27]

166. Likewise, in *The Wall Street Journal*, former fellow at the Open Society Institute (and current principal technologist at the ACLU) Christopher Soghoian noted:

> The dirty secret of the Web is that the "free" content and services that consumers enjoy come with a hidden price: their own private data. Many of the major online advertising companies are not interested in the data that we knowingly and willingly share. Instead, these parasitic firms covertly track our web-browsing activities, search behavior and geolocation information. Once collected, this mountain of data is analyzed to build digital dossiers on millions of consumers, in some cases identifying us by name, gender, age as well as the medical conditions and political issues we have researched online.
>
> Although we now regularly trade our most private information for access to social-networking sites and free content, the terms of this exchange were never clearly communicated to consumers.[28]

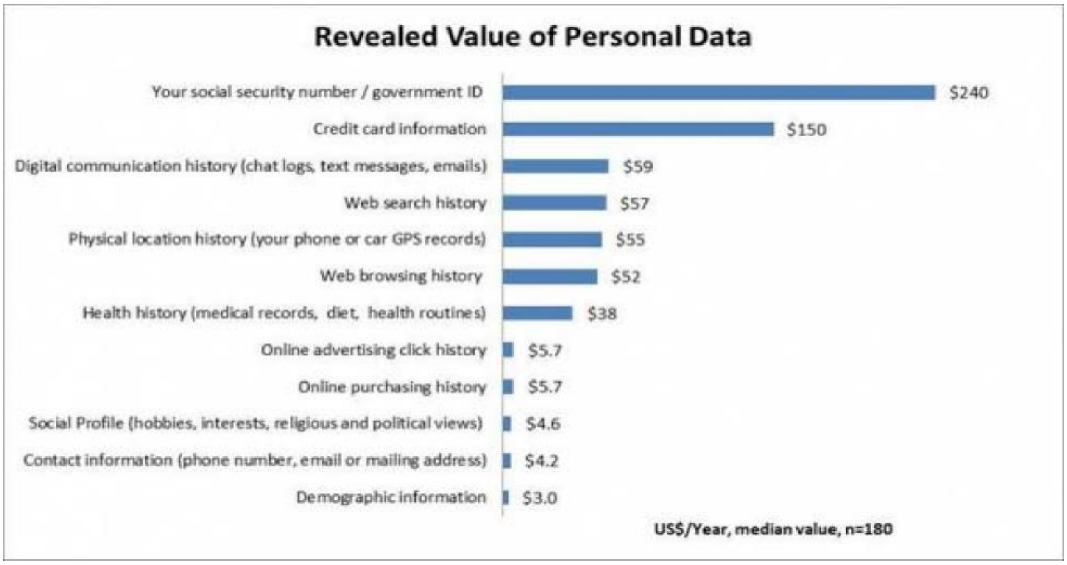
167. The cash value of the personal user information unlawfully collected by Google can be quantified. For example, in a study authored by Tim Morey, researchers studied the value that 180 internet users placed on keeping personal data secure.[29] Contact information of the sort that Google requires was valued by the study participants at approximately $4.20 per year. Demographic information was valued at approximately $3.00 per year. However, web browsing histories were valued at a much higher rate: $52.00 per year. The chart below summarizes the findings:

---

[27] Paul M. Schwartz, *Property, Privacy and Personal Data*, 117 HARV. L. REV. 2055, 2056–57 (2004).

[28] Julia Angwin, *How Much Should People Worry About the Loss of Online Privacy?*, THE WALL STREET JOURNAL (Nov. 15, 2011).

[29] Tim Morey, *What's Your Personal Data Worth?*, DESIGN MIND (Jan. 18, 2011), https://web.archive.org/web/20131206000037/http://designmind.frogdesign.com/blog/what039s-your-personal-data-worth.html.



168. Similarly, the value of user-correlated internet browsing history can be quantified, because Google itself was willing to pay users for the exact type of communications that Google illegally intercepted from Plaintiffs. For example, Google Inc. had a panel (and still has one today) called "Google Screenwise Trends" which, according to the internet giant, is designed "to learn more about how everyday people use the Internet."

169. Upon becoming a panelist, internet users would add a browser extension that shares with Google the sites they visit and how they use them. The panelists consented to Google tracking such information for three months in exchange for one of a number of "gifts," including gift cards to retailers such as Barnes & Noble, Walmart, and Overstock.com.

170. After three months, Google also agreed to pay panelists additional gift cards "for staying with" the panel. These gift cards, mostly valued at exactly $5, demonstrated conclusively that internet industry participants understood the enormous value in internet users' browsing habits. Google has paid Screenwise panelists up to $3 *per week* to be tracked.

171. As demonstrated above, user-correlated URLs have monetary value. They also have non-monetary, privacy value. For example, in a recent study by the Pew Research Center, 93% of Americans said it was "important" for them to be "in control of who can get information" about them. Seventy-four percent said it was "very important." Eighty-seven percent of Americans said it was "important" for them not to have someone watch or listen to them without their permission. Sixty-seven percent said it was "very important." And 90% of Americans said it was

"important" that they be able to "control[] what information is collected about [them]." Sixty-five percent said it was very important.

172. Likewise, in a 2011 Harris Poll study, 76% of Americans agreed that "online companies, such as Google or Facebook, control too much of our personal information and know too much about our browsing habits."

173. Consumers' sensitive and valuable personal information increased as a commodity, where Google itself began paying users specifically for their browsing data.[30] As early as 2012 Google publicly admitted it utilized consumers' browsing data, paired with other sensitive and valuable personal information, to achieve what it called "nowcasting," or "contemporaneous forecasting," which Google's Chief Economist Hal Varian equated to the ability to predict what is happening as it occurs.[31]

174. As the thirst grew for sensitive, personal information,[32] it became readily apparent that the world's most valuable resource was no longer oil, but instead consumers' data in the form of their sensitive, personal information.[33]

175. A number of platforms have appeared where consumers can and do directly monetize their own data, and prevent tech companies from targeting them absent their express

---

[30] Jack Marshall, *Google Pays Users for Browsing Data*, DigiDay (Feb. 10, 2012), https://digiday.com/media/google-pays-users-for-browsing-data/

[31] K.N.C., *Questioning the searches*, The Economist (June 13, 2012), https://www.economist.com/schumpeter/2012/06/13/questioning-the-searchers

[32] *Exploring the Economic of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD Digital Economy Paper No. 220 at 7 (Apr. 2, 2013), http://dx.doi.org/10.1787/5k486qtxldmq-en; *Supporting Investment in Knowledge Capital, Growth and Innovation*, OECD, at 319 (Oct. 13, 2013), https://www.oecd.org/sti/inno/newsourcesofgrowthknowledge-basedcapital.htm; Pauline Glickman and Nicolas Glady, *What's the Value of Your Data?* TechCrunch (Oct. 13, 2015) https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/; Paul Lewis and Paul Hilder, *Former Cambridge Analytica exec says she wants lies to stop*, The Guardian (March 23, 2018) https://www.theguardian.com/uk-news/2018/mar/23/former-cambridge-analytica-executive-brittany-kaiser-wants-to-stop-lies; Shoshanna Zuboff, The Age of Surveillance Capitalism 166 (2019).

[33] *The world's most valuable resource is no longer oil, but data*, The Economist (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

consent:

a. Brave's web browser, for example, will pay users to watch online targeted ads, while blocking out everything else.[34]

b. Loginhood states that it "lets individuals earn rewards for their data and provides website owners with privacy tools for site visitors to control their data sharing," via a "consent manager" that blocks ads and tracking on browsers as a plugin.[35]

c. Ex-presidential candidate Andrew Yang's "Data Dividend Project" aims to help consumers, "[t]ake control of your personal data. If companies are profiting from it, you should get paid for it."[36]

d. Killi is a data exchange platform that allows you to own and earn from your data.[37]

e. Similarly, BIGtoken "is a platform to own and earn from your data. You can use the BIGtoken application to manage your digital data and identity and earn rewards when your data is purchased."[38]

f. The Nielsen Company, famous for tracking the behavior of television viewers' habits, has extended their reach to computers and mobile devices

---

[34] Get Paid to Watch Ads in the Brave Web Browser, at: https://lifehacker.com/get-paid-to-watch-ads-in-the-brave-web-browser-1834332279#:~:text=Brave%2C%20a%20chromium-based%20web%20browser%20that%20boasts%20an,a%20more%20thoughtful%20way%20than%20we%E2%80%99re%20accustomed%20to (Lifehacker, April 26, 2019) ("The model is entirely opt-in, meaning that ads will be disable by default. The ads you view will be converted into Brave's cryptocurrency, Basic Attention Tokens (BAT), paid out to your Brave wallet monthly").

[35] https://loginhood.io/. See also, https://loginhood.io/product/chrome-extension ("[s]tart earning rewards for sharing data – and block others that have been spying on you. Win-win.").

[36] How Does It Work, at: https://www.datadividendproject.com/ ("Get Your Data Dividend…We'll send you $$$ as we negotiate with companies to compensate you for using your personal data.").

[37] https://killi.io/earn/.

[38] https://bigtoken.com/faq#general_0 ("Third-party applications and sites access BIGtoken to learn more about their consumers and earn revenue from data sales made through their platforms. Our BIG promise: all data acquisition is secure and transparent, with consumers made fully aware of how their data is used and who has access to it.").

> through Nielsen Computer and Mobile Panel. By installing the application on your computer, phone, tablet, e-reader, or other mobile device, Nielsen tracks your activity, enters you into sweepstakes with monetary benefits, and earn points worth up to $50 per month.[39]

176. Technology companies recognize the monetary value of users' sensitive, personal information, insofar as they encourage users to install applications explicitly for the purpose of selling that information to technology companies in exchange for monetary benefits.[40]

177. The CCPA recognizes that consumers' personal data is a property right. Not only does the CCPA prohibit covered businesses from discriminating against consumers that opt-out of data collection, the CCPA also expressly provides that: "[a] business may offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale of personal information, or the deletion of personal information." Cal. Civ. Code § 1798.125(b)(1). The CCPA provides that, "[a] business shall not use financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature." Cal. Civ. Code § 1798.125(b)(4).

178. Through its false representations and unlawful data collection, Google is unjustly enriching itself at the cost of consumer choice, when the consumer would otherwise have the ability to choose how they would monetize their own data.

VI. Tolling of the Statute of Limitations

179. Any applicable statutes of limitations have been tolled under (1) the fraudulent concealment doctrine, based on Google's knowing and active concealment and denial of the facts

---

[39] Kevin Mercandante, *Ten Apps for Selling Your Data for Cash*, Best Wallet Hacks (June 10, 2020), https://wallethacks.com/apps-for-selling-your-data/.

[40] Kari Paul, *Google launches app that will pay users for their data*, The Guardian (June 11, 2019), https://www.theguardian.com/technology/2019/jun/11/facebook-user-data-app-privacy-study; Saheli Roy Choudhury and Ryan Browne, *Facebook pays teens to install an app that could collect all kinds of data*, CNBC (Jan. 30, 2019), https://www.cnbc.com/2019/01/29/facebook-paying-users-to-install-app-to-collect-data-techcrunch.html; Jay Peters, *Facebook will now pay you for your voice recordings*, The Verge (Feb. 20, 2020), https://www.theverge.com/2020/2/20/21145584/facebook-pay-record-voice-speech-recognition-viewpoints-prounciations-app.

alleged herein, (2) the delayed discovery doctrine, as Plaintiffs did not and could not reasonably have discovered Google's conduct alleged herein until shortly before the Complaint was filed, (3) the *Brown* Lawsuit, and the assertion there of Plaintiffs' claims, and (4) the terms of the tolling agreement entered into between Plaintiffs (and others) and Google, along with all amendments to that tolling agreement, which expressly tolled the statute of limitations for these claims through the termination of that agreement (and with the filing of this complaint)

180. Google repeatedly and falsely represented that its users (including Plaintiffs) could prevent Google from tracking users and collecting their information, such as by using a browser in "private browsing mode" (including Incognito mode).

181. Google never disclosed that it would continue to track users and collect their data once these steps were performed, nor did Google ever admit that it would still attempt to collect, aggregate, and analyze user data so that it can continue to track individual users even when the user has followed Google's instructions on how to browse privately.

182. Google also further misled users (including Plaintiffs) by indicating that data associated with them would be viewable through their account, but Google did not include the user data at issue in this lawsuit (collected while in a private browser mode) in user accounts. Google's failure to do so is part of Google's active deception and concealment.

183. Google has also made the following statements, which (1) misrepresent material facts about Google's interception and use of users' data in Incognito mode and/or (2) omit to state material facts necessary to make the statements not misleading. Google thereby took affirmative steps to mislead Plaintiffs and other users about the privacy of their data when using private browsing modes like Incognito.

- On September 23, 2014, Google Chairman Eric Schmidt stated during an ABC interview that in Incognito "no one sees anything about you."[41]
- On December 12, 2014, Google Chairman Eric Schmidt stated during a CATO interview that Incognito is browsing "where no information of any kind is

[41] https://abcnews.go.com/Business/video/eric-schmidts-message-tim-cook-25701453

retained about what you're doing."[42]

- On September 27, 2016, Google Director of Product Management Unni Narayana published an article in which he wrote that Google was giving users "more control with incognito mode" and stated: "Your searches are your business. That's why we've added the ability to search privately with incognito mode in the Google app for iOS. When you have incognito mode turned on in your settings, your search and browsing history will not be saved."[43]
- On September 8, 2017, Google Product Manager Greg Fair posted an article titled "Improving our privacy controls with a new Google Dashboard" in which he touted how Google has "[p]owerful privacy controls that work for you" and emphasizing how users had "control" over their information and tools "for controlling your data across Google."[44]
- On May 25, 2018, Google updated its Privacy Policy to state that users are "in control" and "can also choose to browse the web privately using Chrome in Incognito mode."[45]
- On June 21, 2018, Google Product Manager Jon Hannemann posted an article titled "More transparency and control in your Google Account" in which he wrote: "For years, we've built and refined tools to help you easily understand, protect and control your information. As needs around security and privacy evolve, we will continue to improve these important tools to help you control how Google works for you."[46]
- In December 2018, Google CEO Sundar Pichai testified publicly, to Congress, that "For Google services, you have a choice of what information is collected, and

---

[42] https://www.cato.org/events/2014-cato-institute-surveillance-conference
[43] https://blog.google/products/search/the-latest-updates-and-improvements-for/.
[44] https://www.blog.google/topics/safety-security/improving-our-privacy-controls-new-google-dashboard/.
[45] https://policies.google.com/privacy/archive/20171218-20180525?hl=en-US.
[46] https://blog.google/technology/safety-security/more-transparency-and-control-your-google-account/.

we make it transparent." He stated that uses "can decide whether that information is collected" and stored and "clearly see what information we have."[47]

- On May 7, 2019, the New York Times published an opinion piece by Google CEO Sundar Pichai in which he represented that it is "vital for companies to give people clear, individual choices around how their data is used" and that Google focuses on "features that make privacy a reality — for everyone." He specifically referenced Incognito, stating: "For example, we recently brought Incognito mode, the popular feature in Chrome that lets you browse the web without linking any activity to you, to YouTube." He continued: "To make privacy real, we give you clear, meaningful choices around your data."[48]
- On May 7, 2019, during Google's annual I/O conference, Google CEO Sundar Pichai represented that Google's products are "built on a foundation of user trust and privacy" and ensuring "that people have clear, meaningful choices around their data." He specifically referenced Incognito mode in Chrome, stating that Google was bringing Incognito mode to Google Maps: "While in Incognito in Maps, your activity, like the places you search and navigate to, won't be linked to your account."[49]
- On October 2, 2019, Google Director of Product Management, Privacy and Data Protection Office Eric Miraglia published an article titled "Keeping privacy and security simple, for you" in which he touted Google's decision to add Incognito mode to Google Maps, stating: "When you turn on Incognito mode in Maps, your Maps activity on that device, like the places you search for, won't be saved to your Google Account and won't be used to personalize your Maps experience."[50]
- On December 19, 2019, Google Vice President of Product Privacy Rahul Roy-

[47] https://techcrunch.com/2018/12/11/google-ceo-sundar-pichai-thinks-android-users-know-how-much-their-phones-are-tracking-them/.
[48] https://www.nytimes.com/2019/05/07/opinion/google-sundar-pichai-privacy.html.
[49] https://singjupost.com/sundar-pichai-at-google-i-o-2019-keynote-full-transcript/?singlepage=1.
[50] https://blog.google/technology/safety-security/keeping-privacy-and-security-simple-you/.

Chowdhury published an article titled "Putting you in control: our work in privacy this year" in which he noted that Google had "expanded incognito mode across all our apps" as an example of Google's "tools to give you control over your data."[51]

- On January 28, 2020, Google Vice President of Product Privacy Rahul Roy-Chowdhury published an article titled "Data Privacy Day: seven ways we protect your privacy" in which he identified Incognito mode as one of the ways Google keeps "you in control of your privacy" and touted how "Incognito mode has been one of our most popular privacy controls since it launched with Chrome in 2008."[52]
- On or about July 29, 2020, Google submitted written remarks to Congress for testimony by its current CEO Sundar Pichai (who helped develop Google's Chrome browser), which stated: "I've always believed that privacy is a universal right and should be available to everyone and Google is committed to keeping your information safe, treating it responsibly and putting you in control of what you choose to share."[53]

184. The above Google representations were false. Google did not provide users with control and permit them to browse privately, and Google instead continued to intercept users' communications and collect user data while users were in a private browsing mode such as Incognito. These Google representations, at a minimum, omitted material facts that would be necessary to make the statements made not misleading, as they left the false impression that Google did not intercept and collect users' data while they were in private browsing mode.

185. Moreover, Google's labeling of the relevant product as "Incognito" mode and "private" is, in and of itself, misleading absent clear disclosures about the ways in which Google intercepts and uses users' private data.

---

[51] https://blog.google/technology/safety-security/putting-you-in-control-privacy-2019/.
[52] https://blog.google/technology/safety-security/data-privacy-day-seven-ways-we-protect-your-privacy/.
[53] https://docs.house.gov/meetings/JU/JU05/20200729/110883/HHRG-116-JU05-Wstate-PichaiS-20200729.pdf.

186. Plaintiffs relied upon Google's false and misleading representations and omissions that they controlled use of their data through private browsing modes such as Incognito and, based on those misrepresentations, believed that Google was not intercepting and using their private data when they were in such private browsing modes.

187. Plaintiffs did not discover that Google was intercepting and using their data in the ways set forth in this Complaint until shortly before this Complaint was filed. They also could not have reasonably discovered Google's unlawful conduct where some of Google's unlawful conduct (e.g., Google's development and use of detection bits) only became known after the *Brown* Lawsuit was filed.

188. Indeed, even after the *Brown* Lawsuit was filed, Google made other misleading public statements about its data interception and collection practices. For example, Google spokesperson Jose Castaneda was quoted in articles published in June 2020 stating: "Incognito mode in Chrome gives you the choice to browse the internet without your activity being saved to your browser or device. As we clearly state each time you open a new incognito tab, websites might be able to collect information about your browsing activity during your session." Once again, Google left the misleading impression that users' data was not being intercepted and collected without their knowledge and omitted to disclose the ways in which Google actually intercepts and uses user data in private browsing sessions.

189. Additional information regarding Google's illegal misconduct only became available through the *Brown* Lawsuit, where Google continued to make misrepresentations regarding Incognito during the course of the *Brown* Lawsuit. For example, as detailed in the two publicly-available orders sanctioning Google for discovery misconduct, Google concealed information, including regarding Google's efforts to detect Incognito browsing using certain heuristics and detection bits. Google also made representations that were inaccurate concerning how private browsing data is logged by Google.

190. Plaintiffs exercised reasonable diligence to protect their data from interception. Indeed, that is precisely the reason *why* they used Google's "Incognito" mode. They did not discover their claims until consulting with counsel shortly before the filing of this Complaint.

191. Although the *Brown* court denied without prejudice Federal Rule of Civil Procedure 23(b)(3) certification, it certified two classes under Federal Rule of Civil Procedure 23(b)(2). In addition, the *Brown* court is still evaluating whether to grant issue certification under Federal Rule of Civil Procedure 23(c)(4), which was concurrently applied for with the 23(b)-certifications. All claims asserted in this Complaint were also asserted in the *Brown* Lawsuit, and the claims for damages here are all based on facts alleged in the *Brown* Lawsuit, largely unchanged since the *Brown* plaintiffs filed the original complaint on June 2, 2020. Google has, therefore, been on notice for over three years of the specific factual allegations made in this Complaint and bringing this action. Plaintiffs clearly bring these claims in good faith.

FACTUAL ALLEGATIONS REGARDING THE NAMED PLAINTIFFS

192. Plaintiff Luna is an adult domiciled in CA and has an active Google account and had an active Google account at all relevant times hereto.

193. Plaintiff Luna accessed the internet and sent and received communications with Websites on several computing devices that were not shared devices, including using Incognito mode in Chrome to visit non-Google websites without being signed into any Google account.

194. Although Plaintiff Luna did not know it at that time, Plaintiff Luna is now informed and believes that Google was still tracking Plaintiff Luna, via various software and services, without consent or authorization.

195. Google thereby tracked Plaintiff Luna and intercepted Plaintiff Luna's communications with Websites without consent or authorization. Many of these requests were URL requests that revealed what Plaintiff Luna viewed and when.

196. Unlike these other websites that ask for permission to sell data in exchange for consideration, Google never asked for Plaintiff Luna's permission and instead impermissibly intercepted Plaintiff Luna's communications with Websites, and sells information gleaned from such communications. Google's practices irreparably damage Plaintiff Luna's privacy and ability to control Plaintiff Luna's own personal rights and data.

197. Plaintiff Massie is an adult domiciled in CA and has an active Google account and had an active Google account at all relevant times hereto.

198. Plaintiff Massie accessed the internet and sent and received communications with Websites on several computing devices that were not shared devices, including using Incognito mode in Chrome to visit non-Google websites without being signed into any Google account.

199. Although Plaintiff Massie did not know it at that time, Plaintiff Massie is now informed and believes that Google was still tracking Plaintiff Massie, via various software and services, without consent or authorization.

200. Google thereby tracked Plaintiff Massie and intercepted Plaintiff Massie's communications with Websites without consent or authorization. Many of these requests were URL requests that revealed what Plaintiff Massie viewed and when.

201. Unlike these other websites that ask for permission to sell data in exchange for consideration, Google never asked for Plaintiff Massie's permission and instead impermissibly intercepted Plaintiff Massie's communications with Websites, and sells information gleaned from such communications. Google's practices irreparably damage Plaintiff Massie's privacy and ability to control Plaintiff Massie's own personal rights and data.

202. Plaintiff Westbrook is an adult domiciled in CA and has an active Google account and had an active Google account at all relevant times hereto.

203. Plaintiff Westbrook accessed the internet and sent and received communications with Websites on several computing devices that were not shared devices, including using Incognito mode in Chrome to visit non-Google websites without being signed into any Google account.

204. Although Plaintiff Westbrook did not know it at that time, Plaintiff Westbrook is now informed and believes that Google was still tracking Plaintiff Westbrook, via various software and services, without consent or authorization.

205. Google thereby tracked Plaintiff Westbrook and intercepted Plaintiff Westbrook's communications with Websites without consent or authorization. Many of these requests were URL requests that revealed what Plaintiff Westbrook viewed and when.

206. Unlike these other websites that ask for permission to sell data in exchange for consideration, Google never asked for Plaintiff Nico Westbrook's permission and instead

impermissibly intercepted Plaintiff Westbrook's communications with Websites, and sells information gleaned from such communications. Google's practices irreparably damage Plaintiff Westbrook's privacy and ability to control Plaintiff Westbrook's own personal rights and data.

207. Plaintiff Daniels is an adult domiciled in CA and has an active Google account and had an active Google account at all relevant times hereto.

208. Plaintiff Daniels accessed the internet and sent and received communications with Websites on several computing devices that were not shared devices, including using Incognito mode in Chrome to visit non-Google websites without being signed into any Google account.

209. Although Plaintiff Daniels did not know it at that time, Plaintiff Daniels is now informed and believes that Google was still tracking Plaintiff Daniels, via various software and services, without consent or authorization.

210. Google thereby tracked Plaintiff Daniels and intercepted Plaintiff Daniels's communications with Websites without consent or authorization. Many of these requests were URL requests that revealed what Plaintiff Daniels viewed and when.

211. Unlike these other websites that ask for permission to sell data in exchange for consideration, Google never asked for Plaintiff Daniels's permission and instead impermissibly intercepted Plaintiff Daniels's communications with Websites, and sells information gleaned from such communications. Google's practices irreparably damage Plaintiff Daniels's privacy and ability to control Plaintiff Daniels's own personal rights and data.

212. Plaintiff Sonza is an adult domiciled in CA and has an active Google account and had an active Google account at all relevant times hereto.

213. Plaintiff Sonza accessed the internet and sent and received communications with Websites on several computing devices that were not shared devices, including using Incognito mode in Chrome to visit non-Google websites without being signed into any Google account.

214. Although Plaintiff Sonza did not know it at that time, Plaintiff Sonza is now informed and believes that Google was still tracking Plaintiff Sonza, via various software and services, without consent or authorization.

215. Google thereby tracked Plaintiff Sonza and intercepted Plaintiff Sonza's

communications with Websites without consent or authorization. Many of these requests were URL requests that revealed what Plaintiff Sonza viewed and when.

216. Unlike these other websites that ask for permission to sell data in exchange for consideration, Google never asked for Plaintiff Sonza's permission and instead impermissibly intercepted Plaintiff Sonza's communications with Websites, and sells information gleaned from such communications. Google's practices irreparably damage Plaintiff Sonza's privacy and ability to control Plaintiff Sonza's own personal rights and data.

217. Plaintiff Jackson is an adult domiciled in CA and has an active Google account and had an active Google account at all relevant times hereto.

218. Plaintiff Jackson accessed the internet and sent and received communications with Websites on several computing devices that were not shared devices, including using Incognito mode in Chrome to visit non-Google websites without being signed into any Google account.

219. Although Plaintiff Jackson did not know it at that time, Plaintiff Jackson is now informed and believes that Google was still tracking Plaintiff Jackson, via various software and services, without consent or authorization.

220. Google thereby tracked Plaintiff Jackson and intercepted Plaintiff Jackson's communications with Websites without consent or authorization. Many of these requests were URL requests that revealed what Plaintiff Jackson viewed and when.

221. Unlike these other websites that ask for permission to sell data in exchange for consideration, Google never asked for Plaintiff Jackson's permission and instead impermissibly intercepted Plaintiff Jackson's communications with Websites, and sells information gleaned from such communications. Google's practices irreparably damage Plaintiff Jackson's privacy and ability to control Plaintiff Jackson's own personal rights and data.

222. Plaintiff Russell is an adult domiciled in CA and has an active Google account and had an active Google account at all relevant times hereto.

223. Plaintiff Russell accessed the internet and sent and received communications with Websites on several computing devices that were not shared devices, including using Incognito mode in Chrome to visit non-Google websites without being signed into any Google account.

224. Although Plaintiff Russell did not know it at that time, Plaintiff Russell is now informed and believes that Google was still tracking Plaintiff Russell, via various software and services, without consent or authorization.

225. Google thereby tracked Plaintiff Russell and intercepted Plaintiff Russell's communications with Websites without consent or authorization. Many of these requests were URL requests that revealed what Plaintiff Russell viewed and when.

226. Unlike these other websites that ask for permission to sell data in exchange for consideration, Google never asked for Plaintiff Russell's permission and instead impermissibly intercepted Plaintiff Russell's communications with Websites, and sells information gleaned from such communications. Google's practices irreparably damage Plaintiff Russell's privacy and ability to control Plaintiff Russell's own personal rights and data.

227. Plaintiff Gleeson is an adult domiciled in CA and has an active Google account and had an active Google account at all relevant times hereto.

228. Plaintiff Gleeson accessed the internet and sent and received communications with Websites on several computing devices that were not shared devices, including using Incognito mode in Chrome to visit non-Google websites without being signed into any Google account.

229. Although Plaintiff Gleeson did not know it at that time, Plaintiff Gleeson is now informed and believes that Google was still tracking Plaintiff Gleeson, via various software and services, without consent or authorization.

230. Google thereby tracked Plaintiff Gleeson and intercepted Plaintiff Gleeson's communications with Websites without consent or authorization. Many of these requests were URL requests that revealed what Plaintiff Gleeson viewed and when.

231. Unlike these other websites that ask for permission to sell data in exchange for consideration, Google never asked for Plaintiff Gleeson's permission and instead impermissibly intercepted Plaintiff Gleeson's communications with Websites, and sells information gleaned from such communications. Google's practices irreparably damage Plaintiff Gleeson's privacy and ability to control Plaintiff Gleeson's own personal rights and data.

232. Plaintiff Monheim is an adult domiciled in CA and has an active Google account

and had an active Google account at all relevant times hereto.

233. Plaintiff Monheim accessed the internet and sent and received communications with Websites on several computing devices that were not shared devices, including using Incognito mode in Chrome to visit non-Google websites without being signed into any Google account.

234. Although Plaintiff Monheim did not know it at that time, Plaintiff Monheim is now informed and believes that Google was still tracking Plaintiff Monheim, via various software and services, without consent or authorization.

235. Google thereby tracked Plaintiff Monheim and intercepted Plaintiff Monheim's communications with Websites without consent or authorization. Many of these requests were URL requests that revealed what Plaintiff Monheim viewed and when.

236. Unlike these other websites that ask for permission to sell data in exchange for consideration, Google never asked for Plaintiff Monheim's permission and instead impermissibly intercepted Plaintiff Monheim's communications with Websites, and sells information gleaned from such communications. Google's practices irreparably damage Plaintiff Monheim's privacy and ability to control Plaintiff Monheim's own personal rights and data.

237. Plaintiff Dill is an adult domiciled in CA and has an active Google account and had an active Google account at all relevant times hereto.

238. Plaintiff Dill accessed the internet and sent and received communications with Websites on several computing devices that were not shared devices, including using Incognito mode in Chrome to visit non-Google websites without being signed into any Google account.

239. Although Plaintiff Dill did not know it at that time, Plaintiff Dill is now informed and believes that Google was still tracking Plaintiff Dill, via various software and services, without consent or authorization.

240. Google thereby tracked Plaintiff Dill and intercepted Plaintiff Dill's communications with Websites without consent or authorization. Many of these requests were URL requests that revealed what Plaintiff Dill viewed and when.

241. Unlike these other websites that ask for permission to sell data in exchange for

consideration, Google never asked for Plaintiff Dill's permission and instead impermissibly intercepted Plaintiff Dill's communications with Websites, and sells information gleaned from such communications. Google's practices irreparably damage Plaintiff Dill's privacy and ability to control Plaintiff Dill's own personal rights and data.

242. Plaintiff Shofet is an adult domiciled in CA and has an active Google account and had an active Google account at all relevant times hereto.

243. Plaintiff Shofet accessed the internet and sent and received communications with Websites on several computing devices that were not shared devices, including using Incognito mode in Chrome to visit non-Google websites without being signed into any Google account.

244. Although Plaintiff Shofet did not know it at that time, Plaintiff Shofet is now informed and believes that Google was still tracking Plaintiff Shofet, via various software and services, without consent or authorization.

245. Google thereby tracked Plaintiff Shofet and intercepted Plaintiff Shofet's communications with Websites without consent or authorization. Many of these requests were URL requests that revealed what Plaintiff Shofet viewed and when.

246. Unlike these other websites that ask for permission to sell data in exchange for consideration, Google never asked for Plaintiff Shofet's permission and instead impermissibly intercepted Plaintiff Shofet's communications with Websites, and sells information gleaned from such communications. Google's practices irreparably damage Plaintiff Shofet's privacy and ability to control Plaintiff Shofet's own personal rights and data.

247. Plaintiff Jordon is an adult domiciled in CA and has an active Google account and had an active Google account at all relevant times hereto.

248. Plaintiff Jordon accessed the internet and sent and received communications with Websites on several computing devices that were not shared devices, including using Incognito mode in Chrome to visit non-Google websites without being signed into any Google account.

249. Although Plaintiff Jordon did not know it at that time, Plaintiff Jordon is now informed and believes that Google was still tracking Plaintiff Jordon, via various software and services, without consent or authorization.

250. Google thereby tracked Plaintiff Jordon and intercepted Plaintiff Jordon's communications with Websites without consent or authorization. Many of these requests were URL requests that revealed what Plaintiff Jordon viewed and when.

251. Unlike these other websites that ask for permission to sell data in exchange for consideration, Google never asked for Plaintiff Jordon's permission and instead impermissibly intercepted Plaintiff Jordon's communications with Websites, and sells information gleaned from such communications. Google's practices irreparably damage Plaintiff Jordon's privacy and ability to control Plaintiff Jordon's own personal rights and data.

252. Plaintiff Brukner is an adult domiciled in CA and has an active Google account and had an active Google account at all relevant times hereto.

253. Plaintiff Brukner accessed the internet and sent and received communications with Websites on several computing devices that were not shared devices, including using Incognito mode in Chrome to visit non-Google websites without being signed into any Google account.

254. Although Plaintiff Brukner did not know it at that time, Plaintiff Brukner is now informed and believes that Google was still tracking Plaintiff Brukner, via various software and services, without consent or authorization.

255. Google thereby tracked Plaintiff Brukner and intercepted Plaintiff Brukner's communications with Websites without consent or authorization. Many of these requests were URL requests that revealed what Plaintiff Brukner viewed and when.

256. Unlike these other websites that ask for permission to sell data in exchange for consideration, Google never asked for Plaintiff Brukner's permission and instead impermissibly intercepted Plaintiff Brukner's communications with Websites, and sells information gleaned from such communications. Google's practices irreparably damage Plaintiff Brukner's privacy and ability to control Plaintiff Brukner's own personal rights and data.

257. Plaintiff Karvasales is an adult domiciled in CA and has an active Google account and had an active Google account at all relevant times hereto.

258. Plaintiff Karvasales accessed the internet and sent and received communications with Websites on several computing devices that were not shared devices, including using

Incognito mode in Chrome to visit non-Google websites without being signed into any Google account.

259. Although Plaintiff Karvasales did not know it at that time, Plaintiff Karvasales is now informed and believes that Google was still tracking Plaintiff Karvasales, via various software and services, without consent or authorization.

260. Google thereby tracked Plaintiff Karvasales and intercepted Plaintiff Karvasales's communications with Websites without consent or authorization. Many of these requests were URL requests that revealed what Plaintiff Karvasales viewed and when.

261. Unlike these other websites that ask for permission to sell data in exchange for consideration, Google never asked for Plaintiff Karvasales's permission and instead impermissibly intercepted Plaintiff Karvasales's communications with Websites, and sells information gleaned from such communications. Google's practices irreparably damage Plaintiff Karvasales's privacy and ability to control Plaintiff Karvasales's own personal rights and data.

262. Plaintiff Smalt is an adult domiciled in CA and has an active Google account and had an active Google account at all relevant times hereto.

263. Plaintiff Smalt accessed the internet and sent and received communications with Websites on several computing devices that were not shared devices, including using Incognito mode in Chrome to visit non-Google websites without being signed into any Google account.

264. Although Plaintiff Smalt did not know it at that time, Plaintiff Smalt is now informed and believes that Google was still tracking Plaintiff Smalt, via various software and services, without consent or authorization.

265. Google thereby tracked Plaintiff Smalt and intercepted Plaintiff Smalt's communications with Websites without consent or authorization. Many of these requests were URL requests that revealed what Plaintiff Smalt viewed and when.

266. Unlike these other websites that ask for permission to sell data in exchange for consideration, Google never asked for Plaintiff Smalt's permission and instead impermissibly intercepted Plaintiff Smalt's communications with Websites, and sells information gleaned from such communications. Google's practices irreparably damage Plaintiff Smalt's privacy and ability

to control Plaintiff Smalt's own personal rights and data.

267. Plaintiff Ely is an adult domiciled in CA and has an active Google account and had an active Google account at all relevant times hereto.

268. Plaintiff Ely accessed the internet and sent and received communications with Websites on several computing devices that were not shared devices, including using Incognito mode in Chrome to visit non-Google websites without being signed into any Google account.

269. Although Plaintiff Ely did not know it at that time, Plaintiff Ely is now informed and believes that Google was still tracking Plaintiff Ely, via various software and services, without consent or authorization.

270. Google thereby tracked Plaintiff Ely and intercepted Plaintiff Ely's communications with Websites without consent or authorization. Many of these requests were URL requests that revealed what Plaintiff Ely viewed and when.

271. Unlike these other websites that ask for permission to sell data in exchange for consideration, Google never asked for Plaintiff Ely's permission and instead impermissibly intercepted Plaintiff Ely's communications with Websites, and sells information gleaned from such communications. Google's practices irreparably damage Plaintiff Ely's privacy and ability to control Plaintiff Ely's own personal rights and data.

272. Plaintiff Dalen is an adult domiciled in CA and has an active Google account and had an active Google account at all relevant times hereto.

273. Plaintiff Dalen accessed the internet and sent and received communications with Websites on several computing devices that were not shared devices, including using Incognito mode in Chrome to visit non-Google websites without being signed into any Google account.

274. Although Plaintiff Dalen did not know it at that time, Plaintiff Dalen is now informed and believes that Google was still tracking Plaintiff Dalen, via various software and services, without consent or authorization.

275. Google thereby tracked Plaintiff Dalen and intercepted Plaintiff Dalen's communications with Websites without consent or authorization. Many of these requests were URL requests that revealed what Plaintiff Dalen viewed and when.

276. Unlike these other websites that ask for permission to sell data in exchange for consideration, Google never asked for Plaintiff Dalen's permission and instead impermissibly intercepted Plaintiff Dalen's communications with Websites, and sells information gleaned from such communications. Google's practices irreparably damage Plaintiff Dalen's privacy and ability to control Plaintiff Dalen's own personal rights and data.

277. Plaintiff Cornelius is an adult domiciled in CA and has an active Google account and had an active Google account at all relevant times hereto.

278. Plaintiff Cornelius accessed the internet and sent and received communications with Websites on several computing devices that were not shared devices, including using Incognito mode in Chrome to visit non-Google websites without being signed into any Google account.

279. Although Plaintiff Cornelius did not know it at that time, Plaintiff Cornelius is now informed and believes that Google was still tracking Plaintiff Cornelius, via various software and services, without consent or authorization.

280. Google thereby tracked Plaintiff Cornelius and intercepted Plaintiff Cornelius's communications with Websites without consent or authorization. Many of these requests were URL requests that revealed what Plaintiff Cornelius viewed and when.

281. Unlike these other websites that ask for permission to sell data in exchange for consideration, Google never asked for Plaintiff Cornelius's permission and instead impermissibly intercepted Plaintiff Cornelius's communications with Websites, and sells information gleaned from such communications. Google's practices irreparably damage Plaintiff Cornelius's privacy and ability to control Plaintiff Cornelius's own personal rights and data.

282. Plaintiff Botosh is an adult domiciled in CA and has an active Google account and had an active Google account at all relevant times hereto.

283. Plaintiff Botosh accessed the internet and sent and received communications with Websites on several computing devices that were not shared devices, including using Incognito mode in Chrome to visit non-Google websites without being signed into any Google account.

284. Although Plaintiff Botosh did not know it at that time, Plaintiff Botosh is now

informed and believes that Google was still tracking Plaintiff Botosh, via various software and services, without consent or authorization.

285. Google thereby tracked Plaintiff Botosh and intercepted Plaintiff Botosh's communications with Websites without consent or authorization. Many of these requests were URL requests that revealed what Plaintiff Botosh viewed and when.

286. Unlike these other websites that ask for permission to sell data in exchange for consideration, Google never asked for Plaintiff Botosh's permission and instead impermissibly intercepted Plaintiff Botosh's communications with Websites, and sells information gleaned from such communications. Google's practices irreparably damage Plaintiff Botosh's privacy and ability to control Plaintiff Botosh's own personal rights and data.

287. Plaintiff Adams is an adult domiciled in CA and has an active Google account and had an active Google account at all relevant times hereto.

288. Plaintiff Adams accessed the internet and sent and received communications with Websites on several computing devices that were not shared devices, including using Incognito mode in Chrome to visit non-Google websites without being signed into any Google account.

289. Although Plaintiff Adams did not know it at that time, Plaintiff Adams is now informed and believes that Google was still tracking Plaintiff Adams, via various software and services, without consent or authorization.

290. Google thereby tracked Plaintiff Adams and intercepted Plaintiff Adams's communications with Websites without consent or authorization. Many of these requests were URL requests that revealed what Plaintiff Adams viewed and when.

291. Unlike these other websites that ask for permission to sell data in exchange for consideration, Google never asked for Plaintiff Adams's permission and instead impermissibly intercepted Plaintiff Adams's communications with Websites, and sells information gleaned from such communications. Google's practices irreparably damage Plaintiff Adams's privacy and ability to control Plaintiff Adams's own personal rights and data.

292. Plaintiff Ornelas is an adult domiciled in CA and has an active Google account and had an active Google account at all relevant times hereto.

293. Plaintiff Ornelas accessed the internet and sent and received communications with Websites on several computing devices that were not shared devices, including using Incognito mode in Chrome to visit non-Google websites without being signed into any Google account.

294. Although Plaintiff Ornelas did not know it at that time, Plaintiff Ornelas is now informed and believes that Google was still tracking Plaintiff Ornelas, via various software and services, without consent or authorization.

295. Google thereby tracked Plaintiff Ornelas and intercepted Plaintiff Ornelas's communications with Websites without consent or authorization. Many of these requests were URL requests that revealed what Plaintiff Ornelas viewed and when.

296. Unlike these other websites that ask for permission to sell data in exchange for consideration, Google never asked for Plaintiff Ornelas's permission and instead impermissibly intercepted Plaintiff Ornelas's communications with Websites, and sells information gleaned from such communications. Google's practices irreparably damage Plaintiff Ornelas's privacy and ability to control Plaintiff Ornelas's own personal rights and data.

297. Plaintiff Powell is an adult domiciled in CA and has an active Google account and had an active Google account at all relevant times hereto.

298. Plaintiff Powell accessed the internet and sent and received communications with Websites on several computing devices that were not shared devices, including using Incognito mode in Chrome to visit non-Google websites without being signed into any Google account.

299. Although Plaintiff Powell did not know it at that time, Plaintiff Powell is now informed and believes that Google was still tracking Plaintiff Powell, via various software and services, without consent or authorization.

300. Google thereby tracked Plaintiff Powell and intercepted Plaintiff Powell's communications with Websites without consent or authorization. Many of these requests were URL requests that revealed what Plaintiff Powell viewed and when.

301. Unlike these other websites that ask for permission to sell data in exchange for consideration, Google never asked for Plaintiff Powell's permission and instead impermissibly intercepted Plaintiff Powell's communications with Websites, and sells information gleaned from

such communications. Google's practices irreparably damage Plaintiff Powell's privacy and ability to control Plaintiff Powell's own personal rights and data.

302. Plaintiff Mansoni is an adult domiciled in CA and has an active Google account and had an active Google account at all relevant times hereto.

303. Plaintiff Mansoni accessed the internet and sent and received communications with Websites on several computing devices that were not shared devices, including using Incognito mode in Chrome to visit non-Google websites without being signed into any Google account.

304. Although Plaintiff Mansoni did not know it at that time, Plaintiff Mansoni is now informed and believes that Google was still tracking Plaintiff Mansoni, via various software and services, without consent or authorization.

305. Google thereby tracked Plaintiff Mansoni and intercepted Plaintiff Mansoni's communications with Websites without consent or authorization. Many of these requests were URL requests that revealed what Plaintiff Mansoni viewed and when.

306. Unlike these other websites that ask for permission to sell data in exchange for consideration, Google never asked for Plaintiff Mansoni's permission and instead impermissibly intercepted Plaintiff Mansoni's communications with Websites, and sells information gleaned from such communications. Google's practices irreparably damage Plaintiff Mansoni's privacy and ability to control Plaintiff Mansoni's own personal rights and data.

307. Plaintiff Pierotti is an adult domiciled in CA and has an active Google account and had an active Google account at all relevant times hereto.

308. Plaintiff Pierotti accessed the internet and sent and received communications with Websites on several computing devices that were not shared devices, including using Incognito mode in Chrome to visit non-Google websites without being signed into any Google account.

309. Although Plaintiff Pierotti did not know it at that time, Plaintiff Pierotti is now informed and believes that Google was still tracking Plaintiff Pierotti, via various software and services, without consent or authorization.

310. Google thereby tracked Plaintiff Pierotti and intercepted Plaintiff Pierotti's communications with Websites without consent or authorization. Many of these requests were

URL requests that revealed what Plaintiff Pierotti viewed and when.

311. Unlike these other websites that ask for permission to sell data in exchange for consideration, Google never asked for Plaintiff Pierotti's permission and instead impermissibly intercepted Plaintiff Pierotti's communications with Websites, and sells information gleaned from such communications. Google's practices irreparably damage Plaintiff Pierotti's privacy and ability to control Plaintiff Pierotti's own personal rights and data.

312. Plaintiff Quinones is an adult domiciled in CA and has an active Google account and had an active Google account at all relevant times hereto.

313. Plaintiff Quinones accessed the internet and sent and received communications with Websites on several computing devices that were not shared devices, including using Incognito mode in Chrome to visit non-Google websites without being signed into any Google account.

314. Although Plaintiff Quinones did not know it at that time, Plaintiff Quinones is now informed and believes that Google was still tracking Plaintiff Quinones, via various software and services, without consent or authorization.

315. Google thereby tracked Plaintiff Quinones and intercepted Plaintiff Quinones's communications with Websites without consent or authorization. Many of these requests were URL requests that revealed what Plaintiff Quinones viewed and when.

316. Unlike these other websites that ask for permission to sell data in exchange for consideration, Google never asked for Plaintiff Quinones's permission and instead impermissibly intercepted Plaintiff Nagle's communications with Websites, and sells information gleaned from such communications. Google's practices irreparably damage Plaintiff Quinones's privacy and ability to control Plaintiff Quinones's own personal rights and data.

317. Plaintiff Degraw is an adult domiciled in CA and has an active Google account and had an active Google account at all relevant times hereto.

318. Plaintiff Degraw accessed the internet and sent and received communications with Websites on several computing devices that were not shared devices, including using Incognito mode in Chrome to visit non-Google websites without being signed into any Google account.

319. Although Plaintiff Degraw did not know it at that time, Plaintiff Degraw is now informed and believes that Google was still tracking Plaintiff Degraw, via various software and services, without consent or authorization.

320. Google thereby tracked Plaintiff Degraw and intercepted Plaintiff Degraw's communications with Websites without consent or authorization. Many of these requests were URL requests that revealed what Plaintiff Degraw viewed and when.

321. Unlike these other websites that ask for permission to sell data in exchange for consideration, Google never asked for Plaintiff Degraw's permission and instead impermissibly intercepted Plaintiff Degraw's communications with Websites, and sells information gleaned from such communications. Google's practices irreparably damage Plaintiff Degraw's privacy and ability to control Plaintiff Degraw's own personal rights and data.

322. Plaintiff Nagle is an adult domiciled in CA and has an active Google account and had an active Google account at all relevant times hereto.

323. Plaintiff Nagle accessed the internet and sent and received communications with Websites on several computing devices that were not shared devices, including using Incognito mode in Chrome to visit non-Google websites without being signed into any Google account.

324. Although Plaintiff Nagle did not know it at that time, Plaintiff Nagle is now informed and believes that Google was still tracking Plaintiff Nagle, via various software and services, without consent or authorization.

325. Google thereby tracked Plaintiff Nagle and intercepted Plaintiff Nagle's communications with Websites without consent or authorization. Many of these requests were URL requests that revealed what Plaintiff Nagle viewed and when.

326. Unlike these other websites that ask for permission to sell data in exchange for consideration, Google never asked for Plaintiff Nagle's permission and instead impermissibly intercepted Plaintiff Nagle's communications with Websites, and sells information gleaned from such communications. Google's practices irreparably damage Plaintiff Nagle's privacy and ability to control Plaintiff Nagle's own personal rights and data.

327. Plaintiff Salgado is an adult domiciled in CA and has an active Google account and

had an active Google account at all relevant times hereto.

328. Plaintiff Salgado accessed the internet and sent and received communications with Websites on several computing devices that were not shared devices, including using Incognito mode in Chrome to visit non-Google websites without being signed into any Google account.

329. Although Plaintiff Salgado did not know it at that time, Plaintiff Salgado is now informed and believes that Google was still tracking Plaintiff Salgado, via various software and services, without consent or authorization.

330. Google thereby tracked Plaintiff Salgado and intercepted Plaintiff Salgado's communications with Websites without consent or authorization. Many of these requests were URL requests that revealed what Plaintiff Salgado viewed and when.

331. Unlike these other websites that ask for permission to sell data in exchange for consideration, Google never asked for Plaintiff Salgado's permission and instead impermissibly intercepted Plaintiff Salgado's communications with Websites, and sells information gleaned from such communications. Google's practices irreparably damage Plaintiff Salgado's privacy and ability to control Plaintiff Salgado's own personal rights and data.

332. Plaintiff Helms is an adult domiciled in CA and has an active Google account and had an active Google account at all relevant times hereto.

333. Plaintiff Helms accessed the internet and sent and received communications with Websites on several computing devices that were not shared devices, including using Incognito mode in Chrome to visit non-Google websites without being signed into any Google account.

334. Although Plaintiff Helms did not know it at that time, Plaintiff Helms is now informed and believes that Google was still tracking Plaintiff Helms, via various software and services, without consent or authorization.

335. Google thereby tracked Plaintiff Helms and intercepted Plaintiff Helms's communications with Websites without consent or authorization. Many of these requests were URL requests that revealed what Plaintiff Helms viewed and when.

336. Unlike these other websites that ask for permission to sell data in exchange for consideration, Google never asked for Plaintiff Helms's permission and instead impermissibly

intercepted Plaintiff Helms's communications with Websites, and sells information gleaned from such communications. Google's practices irreparably damage Plaintiff Helms's privacy and ability to control Plaintiff Helms's own personal rights and data.

337. Plaintiff Dugger is an adult domiciled in CA and has an active Google account and had an active Google account at all relevant times hereto.

338. Plaintiff Dugger accessed the internet and sent and received communications with Websites on several computing devices that were not shared devices, including using Incognito mode in Chrome to visit non-Google websites without being signed into any Google account.

339. Although Plaintiff Dugger did not know it at that time, Plaintiff Dugger is now informed and believes that Google was still tracking Plaintiff Dugger, via various software and services, without consent or authorization.

340. Google thereby tracked Plaintiff Dugger and intercepted Plaintiff Dugger's communications with Websites without consent or authorization. Many of these requests were URL requests that revealed what Plaintiff Dugger viewed and when.

341. Unlike these other websites that ask for permission to sell data in exchange for consideration, Google never asked for Plaintiff Dugger's permission and instead impermissibly intercepted Plaintiff Dugger's communications with Websites, and sells information gleaned from such communications. Google's practices irreparably damage Plaintiff Dugger privacy and ability to control Plaintiff Dugger's own personal rights and data.

342. Plaintiff Masri is an adult domiciled in CA and has an active Google account and had an active Google account at all relevant times hereto.

343. Plaintiff Masri accessed the internet and sent and received communications with Websites on several computing devices that were not shared devices, including using Incognito mode in Chrome to visit non-Google websites without being signed into any Google account.

344. Although Plaintiff Masri did not know it at that time, Plaintiff Masri is now informed and believes that Google was still tracking Plaintiff Masri, via various software and services, without consent or authorization.

345. Google thereby tracked Plaintiff Masri and intercepted Plaintiff Masri's

communications with Websites without consent or authorization. Many of these requests were URL requests that revealed what Plaintiff Masri viewed and when.

346. Unlike these other websites that ask for permission to sell data in exchange for consideration, Google never asked for Plaintiff Masri's permission and instead impermissibly intercepted Plaintiff Masri's communications with Websites, and sells information gleaned from such communications. Google's practices irreparably damage Plaintiff Masri's privacy and ability to control Plaintiff Masri's own personal rights and data.

347. Plaintiff Corona is an adult domiciled in CA and has an active Google account and had an active Google account at all relevant times hereto.

348. Plaintiff Corona accessed the internet and sent and received communications with Websites on several computing devices that were not shared devices, including using Incognito mode in Chrome to visit non-Google websites without being signed into any Google account.

349. Although Plaintiff Corona did not know it at that time, Plaintiff Corona is now informed and believes that Google was still tracking Plaintiff Corona, via various software and services, without consent or authorization.

350. Google thereby tracked Plaintiff Corona and intercepted Plaintiff Corona's communications with Websites without consent or authorization. Many of these requests were URL requests that revealed what Plaintiff Corona viewed and when.

351. Unlike these other websites that ask for permission to sell data in exchange for consideration, Google never asked for Plaintiff Corona's permission and instead impermissibly intercepted Plaintiff Corona's communications with Websites, and sells information gleaned from such communications. Google's practices irreparably damage Plaintiff Corona's privacy and ability to control Plaintiff Corona's own personal rights and data.

352. Plaintiff Cardamone is an adult domiciled in CA and has an active Google account and had an active Google account at all relevant times hereto.

353. Plaintiff Cardamone accessed the internet and sent and received communications with Websites on several computing devices that were not shared devices, including using Incognito mode in Chrome to visit non-Google websites without being signed into any Google

account.

354. Although Plaintiff Cardamone did not know it at that time, Plaintiff Cardamone is now informed and believes that Google was still tracking Plaintiff Cardamone, via various software and services, without consent or authorization.

355. Google thereby tracked Plaintiff Cardamone and intercepted Plaintiff Cardamone's communications with Websites without consent or authorization. Many of these requests were URL requests that revealed what Plaintiff Cardamone viewed and when.

356. Unlike these other websites that ask for permission to sell data in exchange for consideration, Google never asked for Plaintiff Cardamone's permission and instead impermissibly intercepted Plaintiff Cardamone's communications with Websites, and sells information gleaned from such communications. Google's practices irreparably damage Plaintiff Cardamone's privacy and ability to control Plaintiff Cardamone's own personal rights and data.

357. Plaintiff Anderson is an adult domiciled in CA and has an active Google account and had an active Google account at all relevant times hereto.

358. Plaintiff Anderson accessed the internet and sent and received communications with Websites on several computing devices that were not shared devices, including using Incognito mode in Chrome to visit non-Google websites without being signed into any Google account.

359. Although Plaintiff Anderson did not know it at that time, Plaintiff Anderson is now informed and believes that Google was still tracking Plaintiff Anderson, via various software and services, without consent or authorization.

360. Google thereby tracked Plaintiff Anderson and intercepted Plaintiff Anderson's communications with Websites without consent or authorization. Many of these requests were URL requests that revealed what Plaintiff Anderson viewed and when.

361. Unlike these other websites that ask for permission to sell data in exchange for consideration, Google never asked for Plaintiff Anderson's permission and instead impermissibly intercepted Plaintiff Anderson's communications with Websites, and sells information gleaned from such communications. Google's practices irreparably damage Plaintiff Anderson's privacy

and ability to control Plaintiff Anderson's own personal rights and data.

362. Plaintiff Zanders is an adult domiciled in CA and has an active Google account and had an active Google account at all relevant times hereto.

363. Plaintiff Zanders accessed the internet and sent and received communications with Websites on several computing devices that were not shared devices, including using Incognito mode in Chrome to visit non-Google websites without being signed into any Google account.

364. Although Plaintiff Zanders did not know it at that time, Plaintiff Zanders is now informed and believes that Google was still tracking Plaintiff Zanders, via various software and services, without consent or authorization.

365. Google thereby tracked Plaintiff Zanders and intercepted Plaintiff Zanders's communications with Websites without consent or authorization. Many of these requests were URL requests that revealed what Plaintiff Zanders viewed and when.

366. Unlike these other websites that ask for permission to sell data in exchange for consideration, Google never asked for Plaintiff Zanders's permission and instead impermissibly intercepted Plaintiff Zanders's communications with Websites, and sells information gleaned from such communications. Google's practices irreparably damage Plaintiff Zanders's privacy and ability to control Plaintiff Zanders's own personal rights and data.

367. Plaintiff Apothaker is an adult domiciled in CA and has an active Google account and had an active Google account at all relevant times hereto.

368. Plaintiff Apothaker accessed the internet and sent and received communications with Websites on several computing devices that were not shared devices, including using Incognito mode in Chrome to visit non-Google websites without being signed into any Google account.

369. Although Plaintiff Apothaker did not know it at that time, Plaintiff Apothaker is now informed and believes that Google was still tracking Plaintiff Apothaker, via various software and services, without consent or authorization.

370. Google thereby tracked Plaintiff Apothaker and intercepted Plaintiff Apothaker's communications with Websites without consent or authorization. Many of these requests were

URL requests that revealed what Plaintiff Apothaker viewed and when.

371. Unlike these other websites that ask for permission to sell data in exchange for consideration, Google never asked for Plaintiff Apothaker's permission and instead impermissibly intercepted Plaintiff Apothaker's communications with Websites, and sells information gleaned from such communications. Google's practices irreparably damage Plaintiff Apothaker's privacy and ability to control Plaintiff Apothaker's own personal rights and data.

372. Plaintiff Elliott is an adult domiciled in CA and has an active Google account and had an active Google account at all relevant times hereto.

373. Plaintiff Elliott accessed the internet and sent and received communications with Websites on several computing devices that were not shared devices, including using Incognito mode in Chrome to visit non-Google websites without being signed into any Google account.

374. Although Plaintiff Elliott did not know it at that time, Plaintiff Elliott is now informed and believes that Google was still tracking Plaintiff Elliott, via various software and services, without consent or authorization.

375. Google thereby tracked Plaintiff Elliott and intercepted Plaintiff Elliott's communications with Websites without consent or authorization. Many of these requests were URL requests that revealed what Plaintiff Elliott viewed and when.

376. Unlike these other websites that ask for permission to sell data in exchange for consideration, Google never asked for Plaintiff Elliott's permission and instead impermissibly intercepted Plaintiff Elliott's communications with Websites, and sells information gleaned from such communications. Google's practices irreparably damage Plaintiff Elliott's privacy and ability to control Plaintiff Elliott's own personal rights and data.

377. Plaintiff Steinberg is an adult domiciled in CA and has an active Google account and had an active Google account at all relevant times hereto.

378. Plaintiff Steinberg accessed the internet and sent and received communications with Websites on several computing devices that were not shared devices, including using Incognito mode in Chrome to visit non-Google websites without being signed into any Google account.

379. Although Plaintiff Steinberg did not know it at that time, Plaintiff Steinberg is now informed and believes that Google was still tracking Plaintiff Steinberg, via various software and services, without consent or authorization.

380. Google thereby tracked Plaintiff Steinberg and intercepted Plaintiff Steinberg's communications with Websites without consent or authorization. Many of these requests were URL requests that revealed what Plaintiff Steinberg viewed and when.

381. Unlike these other websites that ask for permission to sell data in exchange for consideration, Google never asked for Plaintiff Steinberg's permission and instead impermissibly intercepted Plaintiff Steinberg's communications with Websites, and sells information gleaned from such communications. Google's practices irreparably damage Plaintiff Steinberg's privacy and ability to control Plaintiff Steinberg's own personal rights and data.

382. Plaintiff Nunez is an adult domiciled in CA and has an active Google account and had an active Google account at all relevant times hereto.

383. Plaintiff Nunez accessed the internet and sent and received communications with Websites on several computing devices that were not shared devices, including using Incognito mode in Chrome to visit non-Google websites without being signed into any Google account.

384. Although Plaintiff Nunez did not know it at that time, Plaintiff Nunez is now informed and believes that Google was still tracking Plaintiff Nunez, via various software and services, without consent or authorization.

385. Google thereby tracked Plaintiff Nunez and intercepted Plaintiff Nunez's communications with Websites without consent or authorization. Many of these requests were URL requests that revealed what Plaintiff Nunez viewed and when.

386. Unlike these other websites that ask for permission to sell data in exchange for consideration, Google never asked for Plaintiff Nunez's permission and instead impermissibly intercepted Plaintiff Nunez's communications with Websites, and sells information gleaned from such communications. Google's practices irreparably damage Plaintiff Nunez's privacy and ability to control Plaintiff Nunez's own personal rights and data.

387. Plaintiff Basche is an adult domiciled in CA and has an active Google account and

had an active Google account at all relevant times hereto.

388. Plaintiff Basche accessed the internet and sent and received communications with Websites on several computing devices that were not shared devices, including using Incognito mode in Chrome to visit non-Google websites without being signed into any Google account.

389. Although Plaintiff Basche did not know it at that time, Plaintiff Basche is now informed and believes that Google was still tracking Plaintiff Basche, via various software and services, without consent or authorization.

390. Google thereby tracked Plaintiff Basche and intercepted Plaintiff Basche's communications with Websites without consent or authorization. Many of these requests were URL requests that revealed what Plaintiff Basche viewed and when.

391. Unlike these other websites that ask for permission to sell data in exchange for consideration, Google never asked for Plaintiff Basche's permission and instead impermissibly intercepted Plaintiff Basche's communications with Websites, and sells information gleaned from such communications. Google's practices irreparably damage Plaintiff Basche's privacy and ability to control Plaintiff Basche's own personal rights and data.

392. Plaintiff Cardona is an adult domiciled in CA and has an active Google account and had an active Google account at all relevant times hereto.

393. Plaintiff Cardona accessed the internet and sent and received communications with Websites on several computing devices that were not shared devices, including using Incognito mode in Chrome to visit non-Google websites without being signed into any Google account.

394. Although Plaintiff Cardona did not know it at that time, Plaintiff Cardona is now informed and believes that Google was still tracking Plaintiff Cardona, via various software and services, without consent or authorization.

395. Google thereby tracked Plaintiff Cardona and intercepted Plaintiff Cardona's communications with Websites without consent or authorization. Many of these requests were URL requests that revealed what Plaintiff Cardona viewed and when.

396. Unlike these other websites that ask for permission to sell data in exchange for consideration, Google never asked for Plaintiff Cardona's permission and instead impermissibly

intercepted Plaintiff Cardona's communications with Websites, and sells information gleaned from such communications. Google's practices irreparably damage Plaintiff Cardona's privacy and ability to control Plaintiff Cardona's own personal rights and data.

397. Plaintiff Herrera is an adult domiciled in CA and has an active Google account and had an active Google account at all relevant times hereto.

398. Plaintiff Herrera accessed the internet and sent and received communications with Websites on several computing devices that were not shared devices, including using Incognito mode in Chrome to visit non-Google websites without being signed into any Google account.

399. Although Plaintiff Herrera did not know it at that time, Plaintiff Herrera is now informed and believes that Google was still tracking Plaintiff Herrera, via various software and services, without consent or authorization.

400. Google thereby tracked Plaintiff Herrera and intercepted Plaintiff Herrera's communications with Websites without consent or authorization. Many of these requests were URL requests that revealed what Plaintiff Herrera viewed and when.

401. Unlike these other websites that ask for permission to sell data in exchange for consideration, Google never asked for Plaintiff Herrera's permission and instead impermissibly intercepted Plaintiff Herrera's communications with Websites, and sells information gleaned from such communications. Google's practices irreparably damage Plaintiff Herrera's privacy and ability to control Plaintiff Herrera's own personal rights and data.

402. Plaintiff Cuellar is an adult domiciled in CA and has an active Google account and had an active Google account at all relevant times hereto.

403. Plaintiff Cuellar accessed the internet and sent and received communications with Websites on several computing devices that were not shared devices, including using Incognito mode in Chrome to visit non-Google websites without being signed into any Google account.

404. Although Plaintiff Cuellar did not know it at that time, Plaintiff Cuellar is now informed and believes that Google was still tracking Plaintiff Cuellar, via various software and services, without consent or authorization.

405. Google thereby tracked Plaintiff Cuellar and intercepted Plaintiff Cuellar's

communications with Websites without consent or authorization. Many of these requests were URL requests that revealed what Plaintiff Cuellar viewed and when.

406. Unlike these other websites that ask for permission to sell data in exchange for consideration, Google never asked for Plaintiff Cuellar's permission and instead impermissibly intercepted Plaintiff Cuellar's communications with Websites, and sells information gleaned from such communications. Google's practices irreparably damage Plaintiff Cuellar's privacy and ability to control Plaintiff Cuellar's own personal rights and data.

407. Plaintiff Valdez is an adult domiciled in CA and has an active Google account and had an active Google account at all relevant times hereto.

408. Plaintiff Valdez accessed the internet and sent and received communications with Websites on several computing devices that were not shared devices, including using Incognito mode in Chrome to visit non-Google websites without being signed into any Google account.

409. Although Plaintiff Valdez did not know it at that time, Plaintiff Valdez is now informed and believes that Google was still tracking Plaintiff Valdez, via various software and services, without consent or authorization.

410. Google thereby tracked Plaintiff Valdez and intercepted Plaintiff Valdez's communications with Websites without consent or authorization. Many of these requests were URL requests that revealed what Plaintiff Valdez viewed and when.

411. Unlike these other websites that ask for permission to sell data in exchange for consideration, Google never asked for Plaintiff Valdez's permission and instead impermissibly intercepted Plaintiff Valdez's communications with Websites, and sells information gleaned from such communications. Google's practices irreparably damage Plaintiff Valdez's privacy and ability to control Plaintiff Valdez's own personal rights and data.

412. Plaintiff Rodriguez is an adult domiciled in CA and has an active Google account and had an active Google account at all relevant times hereto.

413. Plaintiff Rodriguez accessed the internet and sent and received communications with Websites on several computing devices that were not shared devices, including using Incognito mode in Chrome to visit non-Google websites without being signed into any Google

account.

414. Although Plaintiff Rodriguez did not know it at that time, Plaintiff Rodriguez is now informed and believes that Google was still tracking Plaintiff Rodriguez, via various software and services, without consent or authorization.

415. Google thereby tracked Plaintiff Rodriguez and intercepted Plaintiff Rodriguez's communications with Websites without consent or authorization. Many of these requests were URL requests that revealed what Plaintiff Rodriguez viewed and when.

416. Unlike these other websites that ask for permission to sell data in exchange for consideration, Google never asked for Plaintiff Rodriguez's permission and instead impermissibly intercepted Plaintiff Rodriguez's communications with Websites, and sells information gleaned from such communications. Google's practices irreparably damage Plaintiff Rodriguez's privacy and ability to control Plaintiff Rodriguez's own personal rights and data.

417. Plaintiff Chrayah is an adult domiciled in CA and has an active Google account and had an active Google account at all relevant times hereto.

418. Plaintiff Chrayah accessed the internet and sent and received communications with Websites on several computing devices that were not shared devices, including using Incognito mode in Chrome to visit non-Google websites without being signed into any Google account.

419. Although Plaintiff Chrayah did not know it at that time, Plaintiff Chrayah is now informed and believes that Google was still tracking Plaintiff Chrayah, via various software and services, without consent or authorization.

420. Google thereby tracked Plaintiff Chrayah and intercepted Plaintiff Chrayah's communications with Websites without consent or authorization. Many of these requests were URL requests that revealed what Plaintiff Chrayah viewed and when.

421. Unlike these other websites that ask for permission to sell data in exchange for consideration, Google never asked for Plaintiff Chrayah's permission and instead impermissibly intercepted Plaintiff Chrayah's communications with Websites, and sells information gleaned from such communications. Google's practices irreparably damage Plaintiff Chrayah's privacy and ability to control Plaintiff Chrayah's own personal rights and data.

422. Plaintiff Byrd is an adult domiciled in CA and has an active Google account and had an active Google account at all relevant times hereto.

423. Plaintiff Byrd accessed the internet and sent and received communications with Websites on several computing devices that were not shared devices, including using Incognito mode in Chrome to visit non-Google websites without being signed into any Google account.

424. Although Plaintiff Byrd did not know it at that time, Plaintiff Byrd is now informed and believes that Google was still tracking Plaintiff Byrd, via various software and services, without consent or authorization.

425. Google thereby tracked Plaintiff Byrd and intercepted Plaintiff Byrd's communications with Websites without consent or authorization. Many of these requests were URL requests that revealed what Plaintiff Byrd viewed and when.

426. Unlike these other websites that ask for permission to sell data in exchange for consideration, Google never asked for Plaintiff Byrd's permission and instead impermissibly intercepted Plaintiff Byrd's communications with Websites, and sells information gleaned from such communications. Google's practices irreparably damage Plaintiff Byrd's privacy and ability to control Plaintiff Byrd's own personal rights and data.

427. Plaintiff Starzinski is an adult domiciled in CA and has an active Google account and had an active Google account at all relevant times hereto.

428. Plaintiff Starzinski accessed the internet and sent and received communications with Websites on several computing devices that were not shared devices, including using Incognito mode in Chrome to visit non-Google websites without being signed into any Google account.

429. Although Plaintiff Starzinski did not know it at that time, Plaintiff Starzinski is now informed and believes that Google was still tracking Plaintiff Starzinski, via various software and services, without consent or authorization.

430. Google thereby tracked Plaintiff Starzinski and intercepted Plaintiff Starzinski's communications with Websites without consent or authorization. Many of these requests were URL requests that revealed what Plaintiff Starzinski viewed and when.

431. Unlike these other websites that ask for permission to sell data in exchange for consideration, Google never asked for Plaintiff Starzinski's permission and instead impermissibly intercepted Plaintiff Starzinski's communications with Websites, and sells information gleaned from such communications. Google's practices irreparably damage Plaintiff Starzinski's privacy and ability to control Plaintiff Starzinski's own personal rights and data.

432. Plaintiff Bith is an adult domiciled in CA and has an active Google account and had an active Google account at all relevant times hereto.

433. Plaintiff Bith accessed the internet and sent and received communications with Websites on several computing devices that were not shared devices, including using Incognito mode in Chrome to visit non-Google websites without being signed into any Google account.

434. Although Plaintiff Bith did not know it at that time, Plaintiff Bith is now informed and believes that Google was still tracking Plaintiff Bith, via various software and services, without consent or authorization.

435. Google thereby tracked Plaintiff Bith and intercepted Plaintiff Bith's communications with Websites without consent or authorization. Many of these requests were URL requests that revealed what Plaintiff Bith viewed and when.

436. Unlike these other websites that ask for permission to sell data in exchange for consideration, Google never asked for Plaintiff Bith's permission and instead impermissibly intercepted Plaintiff Bith's communications with Websites, and sells information gleaned from such communications. Google's practices irreparably damage Plaintiff Bith's privacy and ability to control Plaintiff Bith's own personal rights and data.

437. Plaintiff Obasa is an adult domiciled in CA and has an active Google account and had an active Google account at all relevant times hereto.

438. Plaintiff Obasa accessed the internet and sent and received communications with Websites on several computing devices that were not shared devices, including using Incognito mode in Chrome to visit non-Google websites without being signed into any Google account.

439. Although Plaintiff Obasa did not know it at that time, Plaintiff Obasa is now informed and believes that Google was still tracking Plaintiff Obasa, via various software and

services, without consent or authorization.

440. Google thereby tracked Plaintiff Obasa and intercepted Plaintiff Obasa's communications with Websites without consent or authorization. Many of these requests were URL requests that revealed what Plaintiff Obasa viewed and when.

441. Unlike these other websites that ask for permission to sell data in exchange for consideration, Google never asked for Plaintiff Obasa's permission and instead impermissibly intercepted Plaintiff Obasa's communications with Websites, and sells information gleaned from such communications. Google's practices irreparably damage Plaintiff Obasa's privacy and ability to control Plaintiff Obasa's own personal rights and data.

442. None of these Plaintiffs consented to or authorized Google's tracking and interception of their confidential communications made while browsing in Incognito mode.

CALIFORNIA LAW APPLIES TO ALL PLAINTIFFS' CLAIMS

443. California's substantive laws apply to every Plaintiff, regardless of where in the United States they reside. Google's Terms of Service explicitly states "California law will govern all disputes arising out of or relating to these terms, service specific additional terms, or any related services, regardless of conflict of laws rules." By choosing California law for the resolution of disputes covered by its Terms of Service, Google concedes that it is appropriate for this Court to apply California law to the instant dispute to all Plaintiffs. Google conceded California law applies to these causes of action in the *Brown* litigation. Plaintiffs are further informed and on that basis allege that Google has consistently forced users of every State to apply California law in their disputes, especially when California law inures to Google's favor.

444. Further, California's substantive laws may be constitutionally applied to the claims of Plaintiffs under the Due Process Clause, *see* U.S. CONST. amend. XIV, § 1, and the Full Faith and Credit Clause, *see* U.S. CONST. art. IV, § 1, of the U.S. Constitution. California has significant contact, or significant aggregation of contacts, to the claims asserted by the Plaintiffs, thereby creating state interests that ensure that the choice of California state law is not arbitrary or unfair. Google's decision to reside in California and avail itself of California's laws, and to engage in the challenged conduct from and emanating out of California, renders the application of California law to the claims

herein constitutionally permissible. The application of California laws to all Plaintiffs is also appropriate under California's choice of law rules because California has significant contacts to the claims of Plaintiffs and California has the greatest interest in applying its laws here.

COUNTS

COUNT ONE: VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT ("CIPA"), CALIFORNIA PENAL CODE §§ 631 AND 632

445. Plaintiffs hereby incorporate Paragraphs 1 through 444 as if fully stated herein.

446. The California Invasion of Privacy Act ("CIPA") is codified at Cal. Penal Code §§ 630 to 638. The Act begins with its statement of purpose:

> The Legislature hereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.

Cal. Penal Code § 630.

447. California Penal Code § 631(a) provides, in pertinent part:

> Any person who, by means of any machine, instrument, or contrivance, or in any other manner . . . willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to lawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine not exceeding two thousand five hundred dollars . . . .

448. California Penal Code § 632(a) provides, in pertinent part:

> A person who, intentionally and without the consent of all parties to a confidential communication, uses an electronic amplifying or recording device to eavesdrop upon or record the confidential communication, whether the communication is carried on among the parties in the presence of one another or by means of a telegraph,

> telephone, or other device, except a radio, shall be punished by a fine not exceeding two thousand five hundred dollars . . . .

449. Under either section of the CIPA, a defendant must show it had the consent of all parties to a communication.

450. Google has its principal place of business in California; designed, contrived and effectuated its scheme to track its users (including Plaintiffs) while they were browsing the internet from a browser while in Incognito mode; and has adopted California substantive law to govern its relationship with its users.

451. To date, Google still "uses, or attempts to use, in any manner, or for any purpose… [the] information [Google] so obtained," including by using information from Plaintiffs' private browsing communications Google surreptitiously intercepted for Google's services and product development, such as for artificial intelligence, machine learning, and advertisement algorithms. Google also continues to "read[], or attempt[] to read, to learn the content" of Plaintiffs' private browsing communications whenever it accesses such stored data.

452. At all relevant times, Google's actual and attempted tracking and interceptions of Plaintiffs' internet communications while using a browser in Incognito mode was without authorization and without consent from the Plaintiffs or Websites. The interception by Google in the aforementioned circumstances were unlawful and tortious.

453. Google's non-consensual actual and attempted tracking and interceptions of Plaintiffs' internet communications who were on their web browser or using a browser in Incognito mode was designed to attempt to learn at least some meaning of the content in the URLs.

454. The following items constitute "machine[s], instrument[s], or contrivance[s]" under the CIPA, and even if they do not, Google's deliberate and admittedly purposeful scheme that facilitated its interceptions falls under the broad statutory catch-all category of "any other manner":

a. The computer codes and programs Google used to track Plaintiffs' communications while they were in Incognito mode;

b. Plaintiffs' browsers and mobile applications;

c. Plaintiffs' computers and mobile devices;

d. Google's servers;

e. The web and ad-servers of websites from which Google tracked and intercepted the Plaintiffs' communications while they were using a web browser in Incognito mode;

f. The computer codes and programs used by Google to effectuate its tracking and interception of Plaintiffs' communications while using the Chrome browser in Incognito mode; and

g. The plan Google carried out to effectuate its tracking and interception of the Plaintiffs' communications while using the Chrome browser in Incognito mode.

455. The data collected by Google constituted "confidential communications," as that term is used in Section 632, because Plaintiffs had objectively reasonable expectations of privacy while browsing in Incognito mode.

456. Plaintiffs have suffered loss by reason of these violations, including, but not limited to, violation of their rights to privacy and loss of value in their personally-identifiable information.

457. Pursuant to California Penal Code § 637.2, Plaintiffs have been injured by the violations of California Penal Code §§ 631 and 632, and each seek damages for the greater of $5,000 per violation or three times the amount of actual damages.

COUNT TWO: VIOLATIONS OF THE COMPREHENSIVE COMPUTER DATA ACCESS AND FRAUD ACT ("CDAFA"), CAL. PENAL CODE § 502 *ET SEQ.*

458. Plaintiffs hereby incorporate Paragraphs 1 through 444 as if fully stated herein.

459. Cal. Penal Code § 502 provides: "For purposes of bringing a civil or a criminal action under this section, a person who causes, by any means, the access of a computer, computer system, or computer network in one jurisdiction from another jurisdiction is deemed to have personally accessed the computer, computer system, or computer network in each jurisdiction." Smart phone devices with the capability of using web browsers are "computers" within the meaning of the statute.

460. Google violated Cal. Penal Code § 502(c)(2) by knowingly accessing and without permission taking, copying, analyzing, and using Plaintiffs' data.

461. Despite Google's false representations to the contrary, Google effectively charged Plaintiffs, and Google was unjustly enriched, by acquiring their sensitive and valuable personal information without permission and using it for Google's own financial benefit to advance its advertising business. Plaintiffs retain a stake in the profits Google earned from their personal browsing histories and other data because, under the circumstances, it is unjust for Google to retain those profits.

462. Google accessed, copied, took, analyzed, and used data from Plaintiffs' computers in and from the State of California, where Google: (1) has its principal place of business; and (2) used servers that provided communication links between Plaintiffs' computers and Google, which allowed Google to access and obtain Plaintiffs' data. Accordingly, Google caused the access of Plaintiffs' computers from California, and is therefore deemed to have accessed Plaintiffs' computers in California.

463. As a direct and proximate result of Google's unlawful conduct within the meaning of Cal. Penal Code § 502, Google has caused loss to Plaintiffs and has been unjustly enriched in an amount to be proven at trial.

464. Plaintiffs seek compensatory damages and/or disgorgement in an amount to be proven at trial.

465. Plaintiffs are entitled to punitive or exemplary damages pursuant to Cal. Penal Code § 502(e)(4) because Google's violations were willful and, upon information and belief, Google is guilty of oppression, fraud, or malice as defined in Cal. Civil Code § 3294.

466. Plaintiffs are also entitled to recover their reasonable attorneys' fees pursuant to Cal. Penal Code § 502(e).

COUNT THREE: INVASION OF PRIVACY

467. Plaintiffs hereby incorporate Paragraphs 1 through 444 as if fully stated herein.

468. The right to privacy in California's constitution creates a right of action against private entities such as Google.

469. Plaintiffs' expectation of privacy is deeply enshrined in California's Constitution. Article I, section 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property and pursuing and obtaining safety, happiness, *and privacy*." The phrase "*and privacy*" was added by the "Privacy Initiative" adopted by California voters in 1972.

470. The phrase "and privacy" was added in 1972 after voters approved a proposed legislative constitutional amendment designated as Proposition 11. Critically, the argument in favor of Proposition 11 reveals that the legislative intent was to curb businesses' control over the unauthorized collection and use of consumers' personal information, stating:

> The right of privacy is the right to be left alone…It prevents government and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us. Fundamental to our privacy is the ability to control circulation of personal information. This is essential to social relationships and personal freedom.[54]

471. The principal purpose of this constitutional right was to protect against unnecessary information gathering, use, and dissemination by public and private entities, including Google.

472. The principal purpose of this constitutional right was to protect against unnecessary information gathering, use, and dissemination by public and private entities, including Google.

473. To plead a California constitutional privacy claim, a plaintiff must show an invasion of (1) a legally protected privacy interest; (2) where the plaintiff had a reasonable expectation of privacy in the circumstances; and (3) conduct by the defendant constituting a serious invasion of privacy.

474. As described herein, Google has intruded upon the following legally protected privacy interests:

a. CIPA as alleged herein;

---

[54] BALLOT PAMP., PROPOSED STATS. & AMENDS. TO CAL. CONST. WITH ARGUMENTS TO VOTERS, GEN. ELECTION *26 (Nov. 7, 1972).

b. A Fourth Amendment right to privacy contained on personal computing devices, including web-browsing history, as explained by the United States Supreme Court in the unanimous decision of *Riley v. California*;

c. The California Constitution, which guarantees Californians the right to privacy;

d. Google's Privacy Policy and policies referenced therein and other public promises it made not to track or intercept the Plaintiffs' communications or access their computing devices and web-browsers while browsing in Incognito mode.

475. Plaintiffs had a reasonable expectation of privacy under the circumstances in that Plaintiffs could not reasonably expect Google would commit acts in violation of civil and criminal laws; and Google affirmatively promised users (including Plaintiffs) it would not track their communications or access their computing devices or web-browsers while they were using a web browser while in Incognito mode.

476. Google's actions constituted a serious invasion of privacy in that it:

a. Invaded a zone of privacy protected by the Fourth Amendment, namely the right to privacy in data contained on personal computing devices, including web search and browsing histories;

b. Violated several criminal laws on interception and invasion of privacy, including CIPA and the CDAFA;

c. Invaded the privacy rights of millions of Americans (including Plaintiffs) without their consent;

d. Constituted the unauthorized taking of valuable information from millions of Americans (including Plaintiffs) through deceit; and

e. Further violated Plaintiffs' reasonable expectation of privacy via Google's review, analysis, and subsequent uses of Plaintiffs' private and other browsing activity that Plaintiffs considered sensitive and confidential.

477. Committing criminal acts against millions of Americans (including Plaintiffs)

constitutes an egregious breach of social norms that is highly offensive.

478. The surreptitious and unauthorized tracking of the internet communications of millions of Americans (including Plaintiffs), particularly where, as here, they have taken active (and recommended) measures to ensure their privacy, constitutes an egregious breach of social norms that is highly offensive.

479. Google's intentional intrusion into Plaintiffs' internet communications and their computing devices and web-browsers was highly offensive to a reasonable person in that Google violated criminal and civil laws designed to protect individual privacy and against theft.

480. The taking of personally-identifiable information from millions of Americans (including Plaintiffs) through deceit is highly offensive behavior.

481. Secret monitoring of web private browsing is highly offensive behavior.

482. Following Google's unauthorized interception of the sensitive and valuable personal information, the subsequent analysis and use of that private browsing activity to target advertising to Plaintiffs violated their reasonable expectations of privacy.

483. Intercepting and surreptitious recording of communications is highly offensive behavior.

484. Google lacked a legitimate business interest in tracking users while they browsed the internet in Incognito mode without their consent. Plaintiffs have been damaged by Google's invasion of their privacy and are entitled to just compensation.

COUNT FOUR: INTRUSION UPON SECLUSION

485. Plaintiffs hereby incorporate Paragraphs 1 through 444 as if fully stated herein.

486. Plaintiffs asserting claims for intrusion upon seclusion must plead (1) intrusion into a private place, conversation, or matter; (2) in a manner highly offensive to a reasonable person.

487. In carrying out its scheme to track and intercept Plaintiffs' communications while they were using a browser while in Incognito mode in violation of its own privacy promises, Google intentionally intruded upon the Plaintiffs' solitude or seclusion in that it effectively placed itself in the middle of conversations to which it was not an authorized party.

488. Google's tracking and interception were not authorized by the Plaintiffs, the

Websites with which they were communicating, or even the Plaintiffs' web-browsers.

489. Google's intentional intrusion into their internet communications and their computing devices and web-browsers was highly offensive to a reasonable person in that they violated criminal and civil laws designed to protect individual privacy and against theft.

490. The taking of personally-identifiable information from millions of Americans (including Plaintiffs) through deceit is highly offensive behavior, particularly where, as here, Plaintiffs took active (and recommended) measures to ensure their privacy.

491. Secret monitoring of web private browsing is highly offensive behavior.

492. Interception and surreptitious recording of communications is highly offensive behavior.

493. Public polling on internet tracking has consistently revealed that the overwhelming majority of Americans believe it is important or very important to be "in control of who can get information" about them; to not be tracked without their consent; and to be in "control[] of what information is collected about [them]." The desire to control one's information is only heightened while a person is browsing the internet in "private browsing mode."

494. Plaintiffs have been damaged by Google's invasion of their privacy and are entitled to reasonable compensation including but not limited to disgorgement of profits related to the unlawful internet tracking.

COUNT FIVE: BREACH OF CONTRACT

495. Plaintiffs hereby incorporate Paragraphs 1 through 444 as if fully stated herein.

496. Google's relationship with its users is governed by the Google Terms of Service, the Google Chrome and Chrome OS Additional Terms of Service, and the Chrome Privacy Notice, which incorporate and/or should be construed consistent with the Privacy Policy, the "Search & Browse Privately" page, and the Incognito Screen.

497. The Chrome Privacy Notice promises Plaintiffs that Google does not collect or use private browsing communications, including by explaining that "[y]ou can limit the information Chrome stores on your system by using incognito mode" and that, within Incognito mode, "Chrome won't store certain information, such as: Basic browsing history information

like URLs, cached paged text, or IP addresses of pages linked from the websites you visit [and] Snapshots of pages that you visit."

498. Google breached these promises.

499. The Privacy Policy, the Incognito Screen, and the "Search & Browse Privately" page similarly promise that users can control Google's collection and use of their browsing data, including by enabling a private browsing mode such as Incognito mode, and that Google would not collect and use private browsing data.

500. Google breached these promises.

501. Plaintiffs fulfilled their obligations under the relevant contracts and are not in breach of any.

502. As a result of Google's breach(es), Google was able to obtain the personal property of Plaintiffs and earn unjust profits.

503. Plaintiffs also did not receive the benefit of the bargain for which they contracted and for which they paid valuable consideration in the form of the personal information they agreed to share, which has ascertainable value to be proven at trial.

504. Plaintiffs seek compensatory damages, consequential damages, and/or non-restitutionary disgorgement in an amount to be proven at trial and any other appropriate relief.

COUNT SIX: CALIFORNIA UNFAIR COMPETITION LAW ("UCL"), CAL. BUS. & PROF. CODE § 17200 *ET SEQ.*

505. Plaintiffs hereby incorporate Paragraphs 1 through 444 as if fully stated herein.

506. The UCL prohibits any "unlawful, unfair, or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising." Cal. Bus. & Prof. Code § 17200 (UCL). By engaging in the practices aforementioned, Google has violated the UCL.

507. Google's "unlawful" acts and practices include its violation of the statutes identified above California Invasion of Privacy Act, Cal. Penal Code §§ 631 and 632; the California Computer Data Access and Fraud Act, Cal. Penal Code § 502, *et seq.*; Invasion of Privacy; Intrusion Upon Seclusion; Breach of Contract; and California Business & Professions Code § 22576.

508. Google's conduct violated the spirit and letter of these laws, which protect property, economic and privacy interests and prohibit unauthorized disclosure and collection of private communications and personal information.

509. Google's "unfair" acts and practices include its violation of property, economic and privacy interests protected by the statutes identified above. To establish liability under the unfair prong, Plaintiffs need not establish that these statutes were actually violated, although the claims pleaded herein do so.

510. Plaintiffs have suffered injury-in-fact, including the loss of money and/or property as a result of Google's unfair and/or unlawful practices, to wit, the unauthorized disclosure and taking of their personal information which has value as demonstrated by its use and sale by Google. Plaintiffs have suffered harm in the form of diminution of the value of their private and personally identifiable data and content.

511. Google's actions caused damage to and loss of Plaintiffs' property right to control the dissemination and use of their personal information and communications.

512. Google reaped unjust profits and revenues in violation of the UCL. This includes Google's profits and revenues from their targeted-advertising and improvements of Google's other products. Plaintiffs seek restitution and disgorgement of these unjust profits and revenues.

COUNT SEVEN: UNJUST ENRICHMENT

513. Plaintiffs hereby incorporate Paragraphs 1 through 444 as if fully stated herein.

514. Plaintiffs conferred upon Google an economic benefit, in the nature of revenues, earnings, and profits, compensation and benefits resulting from Google's unfair and/or unlawful practices described in Paragraphs 1 through 444.

515. Google's financial benefits resulting from its unlawful and inequitable conduct are economically traceable to these unfair and/or unlawful practices.

516. That economic benefit is a direct and proximate result of Google's unfair and/or unlawful practices.

517. This conduct was wrongful, knowing, and conscious.

518. It would be inequitable and unjust for Google to be permitted to retain any of the

unlawful proceeds resulting from its unfair and/or unlawful conduct.

519. As alleged in this Complaint, Google has been unjustly enriched as a result of its wrongful conduct.

520. Plaintiffs are accordingly entitled to equitable relief including restitution and/or non-restitutionary disgorgement of all revenues, earnings, profits, compensation, and benefits which may have been obtained by Google as a result of its unfair and/or unlawful practices, in whole or in part, including through the establishment of a constructive trust.

521. Plaintiffs lack an adequate remedy at law with respect to this claim.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully request that this Court:

A. For all Counts, award damages to Plaintiffs in an amount to be proven at trial, including interest thereon;

B. For Count I, award statutory damages;

C. Non-restitutionary disgorgement of all of Defendant's profits that were derived, in whole or in part, including through the establishment of a constructive trust, from Google's interception and subsequent use of Plaintiffs' communications, including under Counts I, II, III, IV, V, and VII;

D. For Counts I, II, III, and IV, award punitive damages;

E. Ordering Defendant to disgorge all revenues and profits wrongfully obtained, including to be held in a constructive trust;

F. Award nominal damages to Plaintiffs against Defendant;

G. Award Plaintiffs their reasonable costs and expenses incurred in this action, including attorneys' fees and expert fees; and

H. Grant Plaintiffs such further relief as the Court deems appropriate.

JURY TRIAL DEMAND

The Plaintiffs demand a trial by jury of all issues so triable.

Dated: March 28, 2024 **BOIES SCHILLER FLEXNER LLP**

/s/ Mark C. Mao
Mark C. Mao

Mark C. Mao, CA Bar No. 236165
mmao@bsfllp.com
Beko Richardson, CA Bar No. 238027
brichardson@bsfllp.com
Joshua M. Stein, CA Bar No. 298856
jstein@bsfllp.com
BOIES SCHILLER FLEXNER LLP
44 Montgomery St., 41st Floor
San Francisco, CA 94104
Tel.: (415) 293-6800
Fax: (415) 293-6899

David Boies (*pro hac vice* forthcoming)
dboies@bsfllp.com
Alex Boies (*pro hac vice* forthcoming)
aboies@bsfllp.com
BOIES SCHILLER FLEXNER LLP
333 Main Street
Armonk, NY 10504
Tel: (914) 749-8200

James Lee (*pro hac vice* forthcoming)
jwlee@bsfllp.com
BOIES SCHILLER FLEXNER LLP
100 SE 2nd St., 28th Floor
Miami, FL 33131
Tel.: (305) 539-8400
Fax: (303) 539-1307

Alison L. Anderson, CA Bar No. 275334
alanderson@bsfllp.com
Melissa Zonne, CA Bar No. 301581
mzonne@bsfllp.com
M. Logan Wright, CA Bar No. 349004
mwright@bsfllp.com
BOIES SCHILLER FLEXNER LLP
2029 Century Park East, Suite 1520
Los Angeles, CA 90067
Telephone: (213) 629-9040
Facsimile: (213) 629-9022

John A. Yanchunis (*pro hac vice* forthcoming)
jyanchunis@forthepeople.com
Ryan J. McGee (*pro hac vice* forthcoming)
rmcgee@forthepeople.com
MORGAN & MORGAN
201 N. Franklin Street, 7th Floor

Tampa, FL 33602
Tel.: (813) 223-5505

Michael F. Ram, CA Bar No. 104805
mram@forthepeople.com
MORGAN & MORGAN
711 Van Ness Ave, Suite 500
San Francisco, CA 94102
Tel: (415) 358-6913

Attorneys for Plaintiffs